

SIMATIC NET Operating Instructions

SCALANCE W788-1PRO (Access Point)

SCALANCE W788-2PRO (Dual Access Point)

SCALANCE W788-1RR (Access Point iPCF)

SCALANCE W788-2RR (Dual Access Point iPCF)

Preface, Contents

Basic Information on Wireless LAN Communication	1
--	----------

Description of the SCALANCE W78x	2
---	----------

Commissioning	3
----------------------	----------

Configuring the IP Address with the Primary Setup Tool	4
---	----------

Configuration Using the Wizards of Web Based Management	5
--	----------

Configuration Using Web Based Management and the Command Line Interface	6
--	----------

Technical Specifications	7
---------------------------------	----------

Approvals, Appendix, Glossary,
Index

Classification of Safety-Related Notices

This document contains notices which you should observe to ensure your own personal safety, as well as to protect the product and connected equipment. These notices are highlighted in the manual by a warning triangle and are marked as follows according to the level of danger:



Danger

indicates that death or severe personal injury **will** result if proper precautions are not taken.



Warning

indicates that death or severe personal injury **can** result if proper precautions are not taken.



Caution

with warning triangle indicates that minor personal injury can result if proper precautions are not taken.

Caution

without warning triangle indicates that damage to property can result if proper precautions are not taken.

Notice

indicates that an undesirable result or status can occur if the relevant notice is ignored.

Note

highlights important information on the product, using the product, or part of the documentation that is of particular importance and that will be of benefit to the user.

© Copyright Siemens AG, 1998 to 2006 - All rights reserved

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Siemens AG
Automation and Drives
Industrial Communication
Postfach 4848, D-90327 Nürnberg

Disclaimer

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly and any necessary corrections included in subsequent editions. Suggestions for improvement are welcome.

C79000-G8976-C184-07
Technical data subject to change.

Trademarks

SIMATIC®, SIMATIC NET®, SINEC®, SIMATIC NET Networking for Industry® and SCALANCE® are registered trademarks of Siemens AG.

Third parties using for their own purposes any other names in this document which refer to trademarks might infringe upon the rights of the trademark owners.

Safety Instructions Regarding your Product

Before you use the product described here, read the safety instructions below thoroughly.

Personnel Qualification Requirements

Only qualified personnel should be allowed to install and work on this equipment. Qualified personnel as referred to in this manual or in the warning notes are defined as persons who are familiar with the installation, assembly, startup and operation of this product and who possess the relevant qualifications for their work, e.g.:

- Training in or authorization for connecting up, grounding or labeling circuits and devices or systems in accordance with current standards in safety technology
- Training in or authorization for the maintenance and use of suitable safety equipment in accordance with current standards in safety technology
- First aid qualification

Correct Usage of Hardware Products

Please note the following regarding the correct usage of hardware products:

Caution

This device may only be used for the applications described in the catalog or the technical description, and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens.

This product can only function correctly and safely if it is transported, stored, set up, and installed correctly, and operated and maintained as recommended.

Before you use the supplied sample programs or programs you have written yourself, make certain that no injury to persons nor damage to equipment can result in your plant or process.

Prior to Startup

Before putting the product into operation, note the following warning:

Caution

Prior to startup you must observe the instructions in the relevant documentation. For ordering data of the documentation please refer to the catalogs or contact your local SIEMENS representative.

Preface

Validity of the Operating Instructions

These Operating Instructions cover the following products:

- SCALANCE W788-1PRO
- SCALANCE W788-2PRO
- SCALANCE W788-1RR
- SCALANCE W788-2RR

Where the description applies to all products, the name SCALANCE W78x is used. Where the description applies to a specific product, the full name of the product is used.

These operating instructions apply to the following software versions:

- SCALANCE W78x firmware as of Version 3.1
- Primary Setup Tool as of Version 3.1

Purpose of the Operating Instructions

These operating instructions are intended to provide you with the information you require to install, commission and operate the SCALANCE W78x correctly. It explains how to configure the SCALANCE W78x and how to integrate the SCALANCE W78x in a WLAN network.

Orientation in the Documentation

Apart from the operating instructions you are currently reading, the following documentation is also available from SIMATIC NET on the topic of Industrial Wireless LANs:

- **Operating Instructions (compact) SCALANCE W7xx**
This document is supplied with the device on paper and contains a concise summary of the most important information required to use the following products:
 - SCALANCE W788-1PRO
 - SCALANCE W788-2PRO
 - SCALANCE W788-1RR
 - SCALANCE W788-2RR
 - SCALANCE W744-1PRO
 - SCALANCE W746-1PRO
 - SCALANCE W747-1RR
- **Operating Instructions SCALANCE W74x**
The comprehensive documentation for the following products:
 - SCALANCE W744-1PRO
 - SCALANCE W746-1PRO
 - SCALANCE W747-1RR

The document contains all the information for the setup, commissioning and operation of these devices. The SCALANCE W74x is connected to a PC / PLC by an Ethernet cable and allows the attachment of these devices to a wireless network; in other words, it is a gateway from a wired to a wireless network.
- **System Manual Wireless LAN Basics**
This includes not only the description of the physical basics and an outline of the most important IEEE standards but also information on data security and a description of industrial uses of wireless LAN.
You should read this manual if you want to set up WLAN networks with a more complex structure (not only connections between two devices).
- **System Manual RCoax**
This system manual contains both an explanation of the technical basis of leaky feeder cables as well as a description of the SIMATIC NET RCoax components and their functionality. The installation / commissioning and connection of RCoax components is explained.
- **Manual IWLAN/PB Link PNIO Gateway for Industrial Ethernet**
The user documentation for the IWLAN/PB Link. This device is a gateway between IWLAN and PROFIBUS.
- **Operating Instructions CP 7515**
The comprehensive user documentation for the CP 7515 communications processor with all the information required to operate this device.
The CP 7515 is inserted in a CardBus / PC-card (32-bit) slot and allows attachment of the PC/PG to a wireless network.

- **Operating Instructions (compact) CP 7515**
This document is supplied with the device on paper and contains a concise summary of the most important information required to use the CP 7515.
- **Manual CP 1515**
The comprehensive user documentation for the CP 1515 communications processor with all the information required to operate this device.
The CP 1515 is inserted in a PC-card slot (Type II) and allows attachment of the PC/PG to a wireless network.

Biological Compatibility

With regard to the question of whether electromagnetic fields (for example in association with industrial wireless LANs) can put human health at risk, we refer to a publication of BITKOM (German Association for information Technology, Telecommunication and New Media e. V.), dated December 2003:

"The same regulations for the protection of health for all other radio applications also apply to WLAN devices. These regulations are based on the protection concept of ICNIRP² or the corresponding recommendation of the European Council.

The independent German radiation protection commission (SSK) was commissioned by the federal German ministry of the environment to investigate the possible dangers - thermal and non-thermal - resulting from electromagnetic fields and came to the following conclusions³:

"The SSK comes to the conclusion that even after evaluation of the latest scientific literature, there is no new scientific evidence regarding proven adverse effects on health that causes any doubt regarding the scientific evaluation on which the protection concept of the ICNIRP or the European Council recommendation."

The SSK also concludes that below the current limit values, there is also no scientific suspicion of health risks.

This assessment agrees with those of other national and international scientific commissions and of the WHO (www.who.int/emf).

Accordingly and in view of the fact that WLAN devices are significantly below the scientifically established limit values, there are no health risks from the electromagnetic fields of WLAN products.

² International Council on Non-Ionizing Radiation Protection

³ *'Limit Values and Precautionary Measures to Protect the General Public from Electromagnetic Fields'* Recommendation of the Radiation Protection Commission (SSK) with scientific justification, Issue 29, 2001."

You will find further information on this topic under the following URL:
www.bitkom.org

Contents

1	Basic Information on Wireless LAN Communication	13
1.1	Network Structure	13
1.2	WLAN Communication	19
1.2.1	MAC-based Communication.....	19
1.2.2	IP-based Communication	20
2	Description of the SCALANCE W78x	21
3	Commissioning.....	31
3.1	Lightning Protection, Power Supply, and Grounding.....	31
3.2	Assembly and Connectors.....	33
3.3	Cabling for Power Supply and Ethernet	35
3.3.1	General Notes.....	35
3.3.2	Assembling an IE Hybrid Cable 2 x 2 + 4 x 0.34 with an IE IP 67 Hybrid Connector	36
3.3.3	Assembling an IE FC TP Standard Cable 4 x 2 GP or IE FC TP Flexible Cable 4 x 2 GP with an IE IP 67 Hybrid Connector	40
3.3.4	Pinout of the M12 Connector.....	43
3.4	Commissioning with the PRESET PLUG	44
4	Configuring the IP Address with the Primary Setup Tool	47
4.1	Introduction	47
4.2	Installation of the DLC Protocol in Windows XP Professional.....	49
4.3	Installation of the DLC Protocol in Windows 2000 Professional SP2.....	50
4.4	Installing the Primary Setup Tool.....	51
4.5	Working with the Primary Setup Tool	52
4.5.1	Primary Setup Tool via the Command Line.....	56
5	Configuration Using the Wizards of Web Based Management.....	57
5.1	Introduction	57
5.2	Starting Web Based Management and Logging On.....	59
5.2.1	Connection over HTTPS.....	60
5.3	Selecting the Wizards.....	61
5.4	Basic Wizard	63
5.4.1	IP Settings	63
5.4.2	System name.....	65
5.4.3	Country Code.....	66
5.4.4	Wireless Settings in Access Point Mode	67
5.4.5	Wireless Settings in Client Mode.....	68
5.4.6	Adopt MAC Address Settings (Client Mode only).....	69

5.4.7	Channel Settings (only in access point mode)	72
5.4.8	Finish	74
5.5	Security Wizard.....	75
5.5.1	Security Settings.....	76
5.5.2	Security Settings for Management Interfaces	77
5.5.3	Security Settings for SNMP Protocol.....	78
5.5.4	Security Settings for WLAN (Page 1, only in access point mode)	79
5.5.5	Security Settings for WLAN (Page 2)	83
5.5.6	Settings for the Security Level Low	87
5.5.7	Settings for the Security Level Medium in Access Point Mode	88
5.5.8	Settings for Security Level Medium in Client Mode.....	89
5.5.9	Settings for the Security Level High	90
5.5.10	Settings for the Security Level Highest.....	91
5.5.11	The Following Settings Were Made.....	91
5.5.12	Finish	92
5.6	iPCF Wizard.....	93
5.6.1	i Point Coordination Function Settings	93
5.6.2	Security Settings for WLAN	96
5.6.3	Public Security Key for WLAN	97
5.6.4	Finish	98
6	Configuration Using Web Based Management and the Command Line Interface	99
6.1	General Information on Web Based Management and the Command Line Interface	99
6.1.1	Introduction	99
6.1.2	The LED Simulation of Web Based Management.....	100
6.1.3	Working with Web Based Management	101
6.1.4	Command Line Interface (CLI)	102
6.2	The System Menu.....	104
6.2.1	System Information Menu Command	104
6.2.2	IP Settings Menu Command.....	112
6.2.3	Services Menu Command	114
6.2.4	Restart Menu Command.....	116
6.2.5	Event Config Menu Command	118
6.2.6	E-mail Config Menu Command	121
6.2.7	SNMP Config Menu Command	122
6.2.8	Syslog Menu Command	127
6.2.9	SNTP Config Menu Command	130
6.2.10	Fault State Menu Command.....	131
6.2.11	Load & Save Menu Command	132
6.2.12	C-PLUG Menu Command.....	136
6.3	Interfaces Menu	141
6.3.1	Ethernet Menu Command	141
6.3.2	WLAN Menu Command.....	143

6.3.3	Advanced Submenu	149
6.3.4	SSID List Submenu (client mode only).....	156
6.3.5	Advanced G Submenu.....	157
6.3.6	Data Rates Submenu Command (access point mode only)	160
6.3.7	VAP Submenu Command	162
6.4	The Security Menu.....	163
6.4.1	Basic Wireless Menu Command	163
6.4.2	Keys Menu Command	173
6.4.3	ACL Menu Command	174
6.4.4	RADIUS Server Menu Command.....	178
6.4.5	Access Menu Command.....	179
6.5	The Bridge Menu	180
6.5.1	WDS Menu Command.....	181
6.5.2	VLAN Menu Command.....	183
6.5.3	Learning Table Menu Command	192
6.5.4	ARP Table Menu Command.....	192
6.5.5	Spanning Tree Menu Command	192
6.5.6	Storm Threshold Menu Command	202
6.5.7	NAT Menu Command.....	203
6.5.8	IP Mapping Table Menu Command.....	208
6.6	The Filters Menu	210
6.6.1	MAC Filter Menu Command	210
6.6.2	MAC Dir Filter Menu Command	211
6.6.3	Protocol Filter Menu Command.....	212
6.7	The I-Features Menu	213
6.7.1	iQoS Menu Command	213
6.7.2	iPCF Menu Command	215
6.7.3	Forced Roaming on IP Down	219
6.7.4	Link Check Menu Command	220
6.7.5	Redundancy Menu Command.....	222
6.7.6	IP-Alive Menu Command.....	224
6.8	The Information Menu.....	226
6.8.1	Log Table Menu Command	227
6.8.2	Auth Log Menu Command.....	228
6.8.3	Versions Menu Command	229
6.8.4	Client List Menu Command	230
6.8.5	Ethernet Menu Command	232
6.8.6	WLAN Menu Command.....	232
6.8.7	iQoS Menu Command	238
6.8.8	Spanning Tree Menu Command	240
6.8.9	IP, TCP/IP, ICMP, SNMP Menu Command.....	242
6.8.10	Signal Recorder Menu Command	242
7	Technical Specifications / Approvals	248

Approvals	252
Appendix	257
Private MIB Variables of the SCALANCE W78x	257
Designing and Calculating Wireless Systems Based on the Example of RCoax	261
Calculating in Decibels	261
Power Specifications	262
Losses Based on the Example of a 2.4 GHz RCoax Cable	264
Receiver Sensitivity	266
System Calculation Based on the Example of RCoax	267
Glossary	269
Index	273

Basic Information on Wireless LAN Communication

1

1.1 Network Structure

Standalone Configuration with the SCALANCE W78x

This configuration does not require a server and the SCALANCE W78x does not have a connection to a wired Ethernet. Within its transmission range, the SCALANCE W78x forwards data from one WLAN node to another.

The wireless network has a unique name. All the devices exchanging data within this network must be configured with this name.

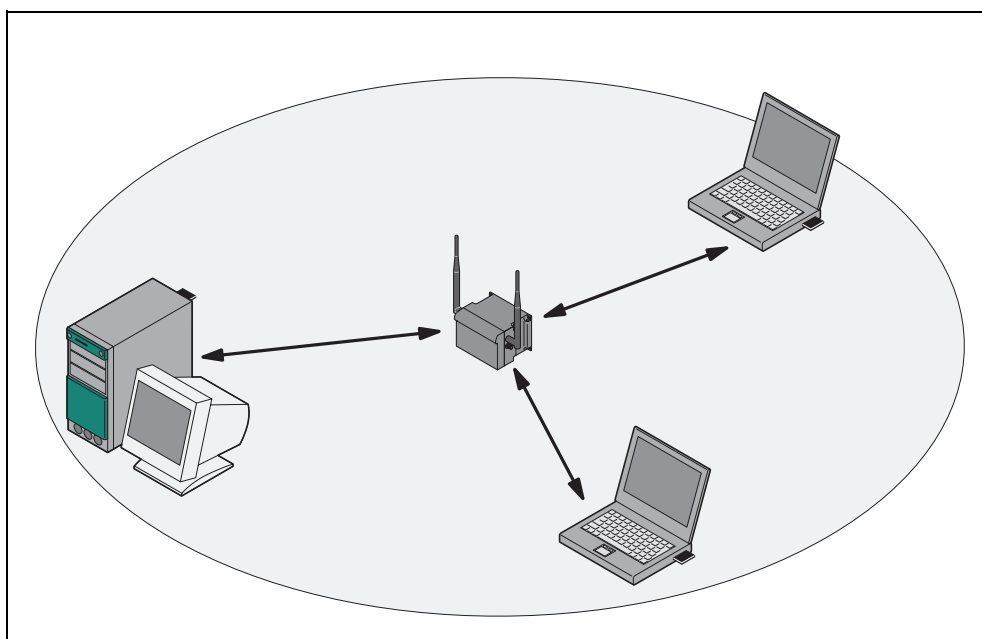


Figure 1-1 Standalone Configuration of a SCALANCE W78x. The gray area indicates the wireless transmission range of the SCALANCE W78x.

Ad Hoc Networks

In the ad hoc mode, nodes communicate directly (connections 1 through 3 in Figure 1-2) without involving a SCALANCE W78x with each other (connection 4). The nodes access common resources (files or even devices, for example a printer) of the server. This is, of course, only possible when the nodes are within the wireless range of the server or within each other's range.

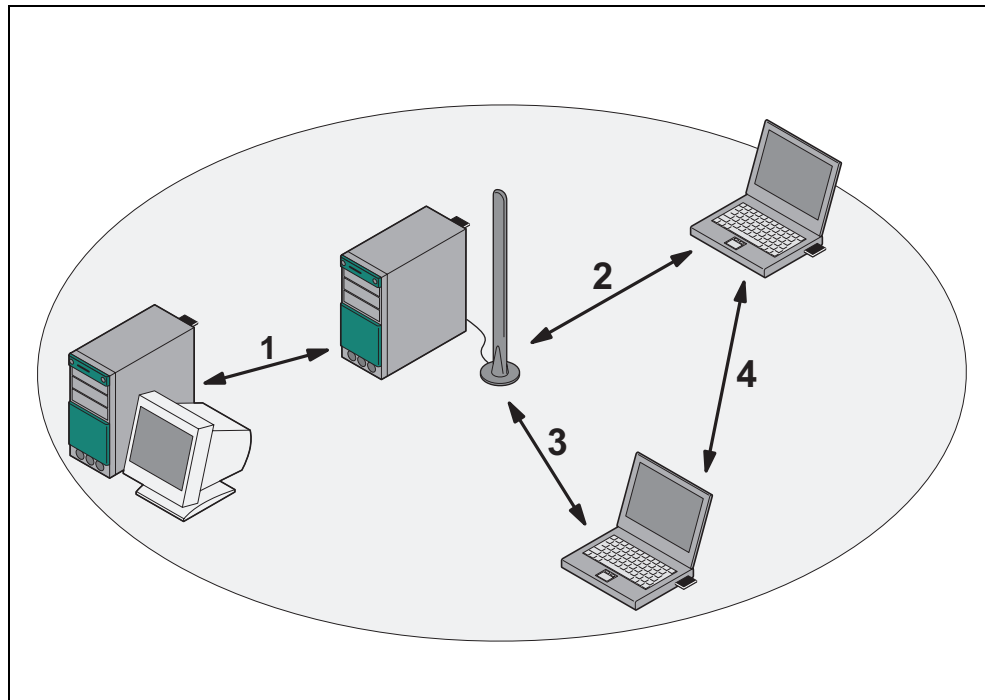


Figure 1-2 Ad Hoc Network without SCALANCE W78x

Wireless Access to a Wired Ethernet Network

If one (or more) SCALANCE W78x access points have access to wired Ethernet, the following applications are possible:

- A single SCALANCE W78x as gateway:
A wireless network can be connected with a wired network over a SCALANCE W78x.
- Span of wireless coverage for the wireless network with several SCALANCE W78x access points:
The SCALANCE W78x access points are all configured with the same unique SSID (network name). All nodes that want to communicate over this network must also be configured with this SSID.

If a mobile station moves from the coverage range (cell) of one SCALANCE W78x to the coverage range (cell) of another SCALANCE W78x, the wireless connection is maintained (this is called roaming).

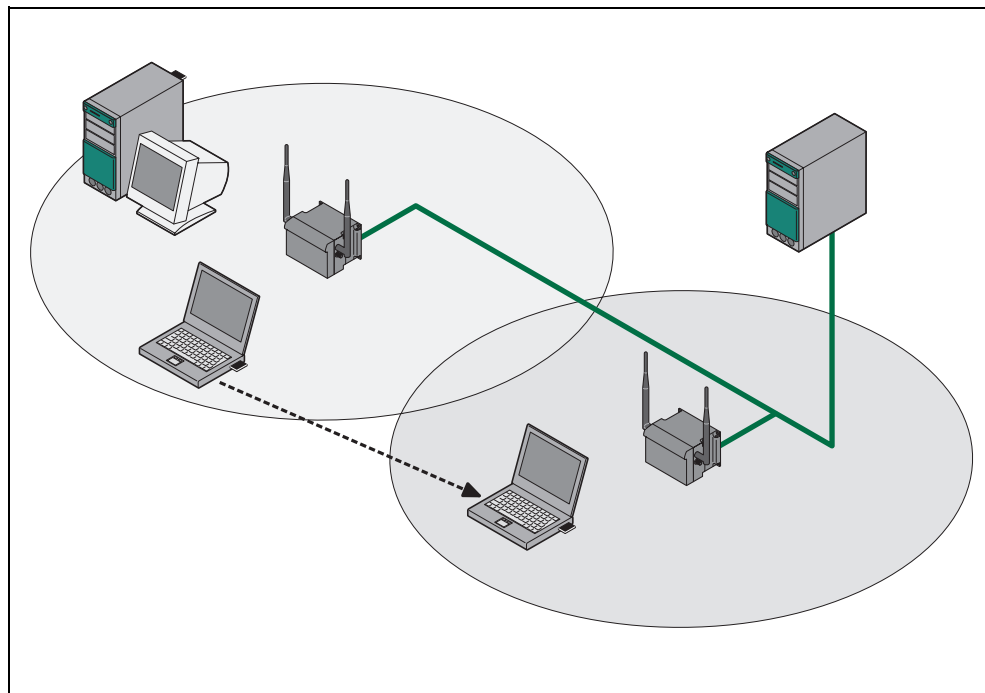


Figure 1-3 Wireless Connection of a Mobile Station over two Cells (Roaming)

Multichannel Configuration

If neighboring SCALANCE W78x access points use the same frequency channel, the response times are longer due to the collisions that occur. If the configuration shown in Figure 1-4 is implemented as a single-channel system, computers A and B cannot communicate at the same time with the SCALANCE W78x access points in their cells.

If neighboring SCALANCE W78x access points are set up for different frequencies, this leads to a considerable improvement in performance. As a result, neighboring cells each have their own medium and the delays resulting from time-offset transmission no longer occur.

Channel spacing should be as large as possible; a practical value would be 25 MHz. Even in a multichannel configuration, all SCALANCE W78x access points can be configured with the same network name.

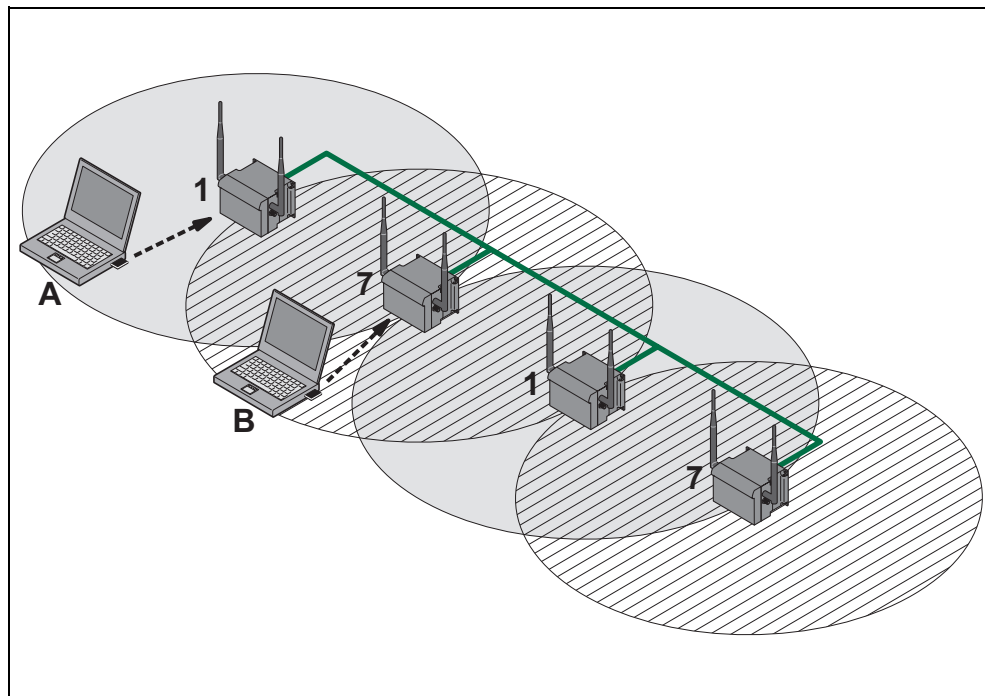


Figure 1-4 Multichannel Configuration on Channels 1 and 7 with four SCALANCE W78x Access Points

Wireless Distribution System (WDS)

WDS allows direct connections between SCALANCE W78x devices and or between SCALANCE W78x and other WDS-compliant devices. These are used to create a wireless backbone or to connect an individual SCALANCE W78x to a network that cannot be connected directly to the cable infrastructure due to its location.

Two alternative configurations are possible. The WDS partner can be configured both using its name and its MAC address.

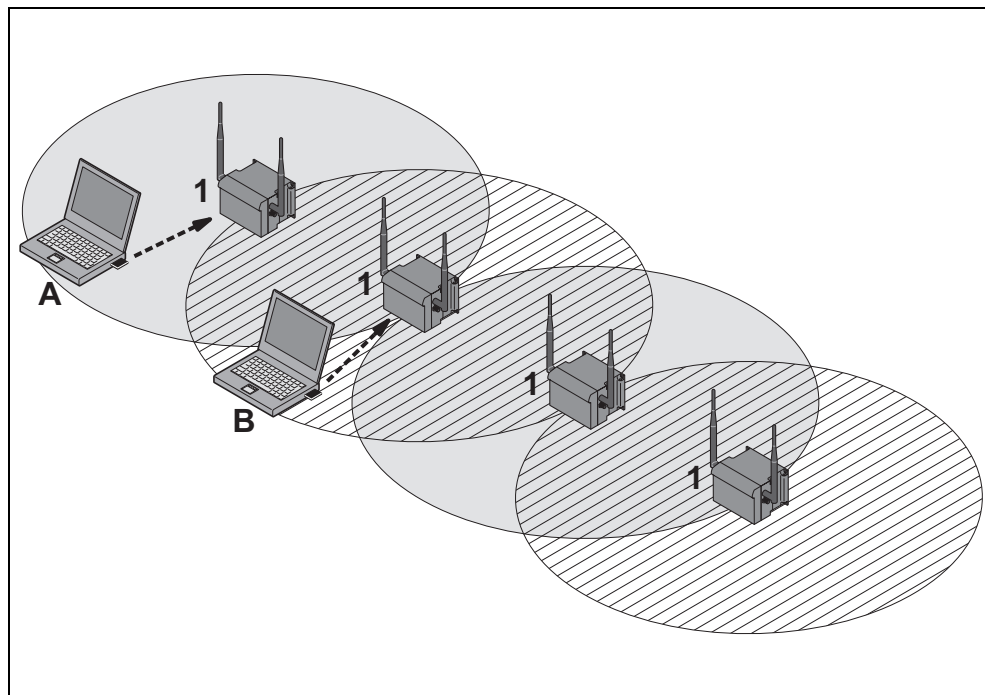


Figure 1-5 Implementation of WDS with four SCALANCE W78x Access Points

Redundant Wireless LAN (RWlan)

RWlan allows a redundant, wireless connection between two SCALANCE W788-2xx devices (W788-2PRO or W788-2RR). This is used to set up a redundant wireless backbone that cannot be implemented as a wired network due to its location but nevertheless has high demands in terms of availability.

Two alternative configurations are possible. The RWlan partner can be configured both using its name and its MAC address.

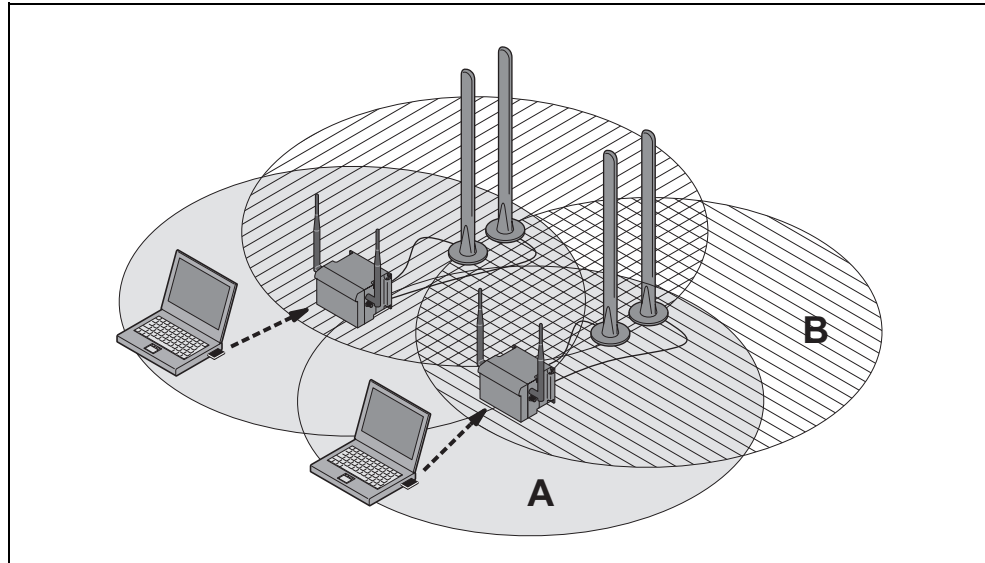


Figure 1-6 Implementation of RWlan with two SCALANCE W788-2xx.
As an alternative, data transfer is possible over one of the two wireless adapters.

1.2 WLAN Communication

1.2.1 MAC-based Communication

Auto Find Adopt MAC / Adopt MAC manually

Frames in the direction from the client to the access point always have the MAC address of the WLAN interface as the source MAC address. As a result, the learning table at the access point end always has only the MAC address of the WLAN interface of the client.

If the MAC address of a device connected to the client over Ethernet is adopted, both the MAC-based and the IP-based frames find their destination in precisely this device.

Other nodes located downstream from the client cannot be reached. The AP checks whether the destination MAC matches the MAC addresses of the connected clients. Since a client can only adopt one MAC address, the access point does not find a match and discards the packets to other nodes.

Maximum possible number of MAC nodes downstream from the client: 1

Notes on setting Auto Find Adopt MAC:

- As long as there is no link on the Ethernet interface, the device uses the MAC address of the Ethernet interface so that it can be reached in this status. In this status, the device can be found using the Primary Setup Tool.
- As soon as there is a link on the Ethernet interface, the device adopts the source MAC address of the first received frame.

Note

From the moment that the device adopts another MAC address (whether manually or automatically), the device no longer responds to queries of the Primary Setup Tool when the query is received over the WLAN interface. Queries of the PST over the Ethernet interface continue to be replied to.

Adopt Own MAC (only W746/W747 and W788 in client mode)

If IP-based frames need to be sent to a device connected downstream from the client, the default setting Adopt Own Mac can be retained. The client registers with the MAC address of its Ethernet adapter. The IP packets are broken down according to an internal table and forwarded to the connected devices (IP mapping).

Communication at the MAC address level (ISO/OSI layer 2) is then only possible with a component downstream from the client if its MAC address was adopted by the client.

Maximum possible number of MAC nodes downstream from the client: 0

Layer 2 Tunneling (only W746/W747 and W788 in client mode)

With layer 2 tunneling, the client provides information about the devices downstream from it when it registers with an access point. This makes it possible to enter the MAC addresses of these devices in the learning table of the access point. The access point can forward MAC-based frames for the devices downstream from the client to the appropriate client.

In much the same way as with WDS, a separate port is created for the L2T client over which the Ethernet frames are sent without changing the destination MAC address.

Maximum possible number of MAC nodes downstream from the client: 8

1.2.2 IP-based Communication

IP Mapping (only W746/747 and W788 in client mode)

If there is more than one device connected downstream from the client and these should only be addressed with IP frames, you can implement WLAN access for several devices with one client. With IP mapping, the client maintains a table with the assignment of MAC address and IP address to forward incoming IP frames to the correct MAC address.

Maximum possible number of IP nodes downstream from the client: 8

Description of the SCALANCE W78x

2

Components of the Product

The following components are supplied with the SCALANCE W78x:

- SCALANCE W78x
- 2 OMNI antennas
- 1 IE IP 67 hybrid plug-in connection
- 1 protective cap for the M12 socket
- 2 (or 4 with SCALANCE W788-2PRO or SCALANCE W788-2RR) protective caps for the R-SMA sockets
- 1 SIMATIC NET Industrial Wireless LAN CD with these Operating Instructions for the SCALANCE W78x

Please check that the consignment you have received is complete. If it is not complete, please contact your supplier or your local Siemens office.

Requirements for Installation and Operation

A PG/PC with a network attachment must be available to configure the SCALANCE W78x. If no DHCP server is available, a PC on which the Primary Setup Tool (PST) is installed is necessary for the initial assignment of an IP address to the SCALANCE W78x. For the other configuration settings, a computer with Telnet or an Internet browser is necessary.

Possible Applications of the SCALANCE W78x

The SCALANCE W78x is equipped with an Ethernet interface and a wireless LAN interface (SCALANCE W788-2PRO and SCALANCE W788-2RR: two WLAN interfaces). This makes the device suitable for the following applications:

- The SCALANCE W78x forwards data within its transmission range from one node to another without a connection to wired Ethernet being necessary.
- The SCALANCE W78x can be used as a gateway from a wired to a wireless network.
- The SCALANCE W78x can be used as a wireless bridge between two networks.
- The SCALANCE W78x can be used as a bridge between two different frequencies.

Over and above this, due to the second interface of the SCALANCE W788-2PRO and the SCALANCE W788-2RR, a redundant wireless link can also be implemented between two SCALANCE W788-2xx modules.

Properties of the SCALANCE W78x

- The Ethernet interface supports 10 Mbps and 100 Mbps, both in full and half duplex as well as autocrossing and autonegotiation.
- Operating the wireless interface in the frequency bands 2.4 GHz and 5 GHz.
- The wireless interface is compatible with the standards IEEE 802.11a , IEEE 802.11b and IEEE 802.11g. In the 802.11a- and 802.11g mode, the gross transmission rate is up to 54 Mbps. In turbo mode, the Transmission rate is up to 108 Mbps (not permitted in all countries and modes).

Note

If the SCALANCE W78x is operated in turbo mode (A, G or H turbo), remember that the channels adjacent to the set transmission channel are also used for communication. Disturbances can therefore occur on these channels when there are neighboring wireless systems. The data throughput can also be reduced if there is competition for use of these channels.

- As an expansion of the 802.11a mode, it is also possible to operated according to the IEEE 802.11h standard. In 802.11h mode, the procedures *Transmit Power Control* (TPC) and *Dynamic Frequency Selection* (DFS) are used in the range 5.25 - 5.35 and 5.47 - 5.75 GHz. This means that in some countries, the frequency sub-band 5.47 - 5.725 GHz can also be used outdoors with higher transmit power.
TPC is a method of controlling the transmit power that is reduced to the currently required level. With dynamic frequency selection (DFS), the access point searches for primary users (for example radar) on a randomly selected channel before starting communication. If signals are found on the channel, this channel is disabled for 30 minutes and the availability check is repeated on another channel.
The gross transmission rate is up to 54 Mbps in 802.11h mode.
- Support of the authentication standards WPA, WPA-PSK, WPA2, WPA2-PSK and IEEE 802.1x and the encryption methods WEP, AES and TKIP.
- Suitable for inclusion of a RADIUS server for authentication.
- Device-related and application-related monitoring of the wireless connection.
- The interoperability of SCALANCE W78x devices with Wi-Fi devices of other vendors was tested thoroughly.
- Only for W78x-1RR/2RR: The iPCF mode provides an optimized data throughput and minimum handover times.

Note

In the client mode, you can use a SCALANCE W788-xRR as SCALANCE W747-1RR and a SCALANCE W788-xPRO as SCALANCE W746-1PRO.

Note

For PNIO communication, we always recommend that you enable the iPCF mode.

The following table illustrates the differences between the various variants of the SCALANCE W78x:

Type	No. of WLAN interfaces		No. of supported IP nodes ⁽³⁾		No. of supported MAC nodes ⁽³⁾		iPCF mode ⁽¹⁾	Order no.
	1	2	1	several	1	several		
W788-1PRO	•			•		•		6GK5788-1ST00-2AA6 6GK5788-1ST00-2AB6 ⁽²⁾
W788-2PRO		•		•		•		6GK5788-2ST00-2AA6 6GK5788-2ST00-2AB6 ⁽²⁾
W788-1RR	•			•		•	•	6GK5788-1SR00-2AA6 6GK5788-1SR00-2AB6 ⁽²⁾
W788-2RR		•		•		•	•	6GK5788-2SR00-2AA6 6GK5788-2SR00-2AB6 ⁽²⁾

(1) The iPCF mode provides an optimized data throughput and minimum handover times.

(2) US variant

(3) In client mode.

In the SCALANCE W78x *HELP* function, you will find further information on the configuration parameters of the relevant device.

Ports

The SCALANCE W78x has the following ports:

- RJ-45 hybrid connector on the front panel of the housing consisting of an RJ-45 jack and 4-pin power socket. The RJ-45 connector supports the use of switches capable of power-over-Ethernet according to 802.3af. The 4-pin power socket allows power of 18 - 32 V DC.
- An M12 connector as optional power supply (18 - 32 V DC).
- Two R-SMA plugs (four R-SMA plugs on the SCALANCE W788-2PRO and SCALANCE W788-2RR) for the attachment of antennas on the sides of the device.

LED Display

On the front of the housing, several LEDs provide information on the operating status of the SCALANCE W78x:

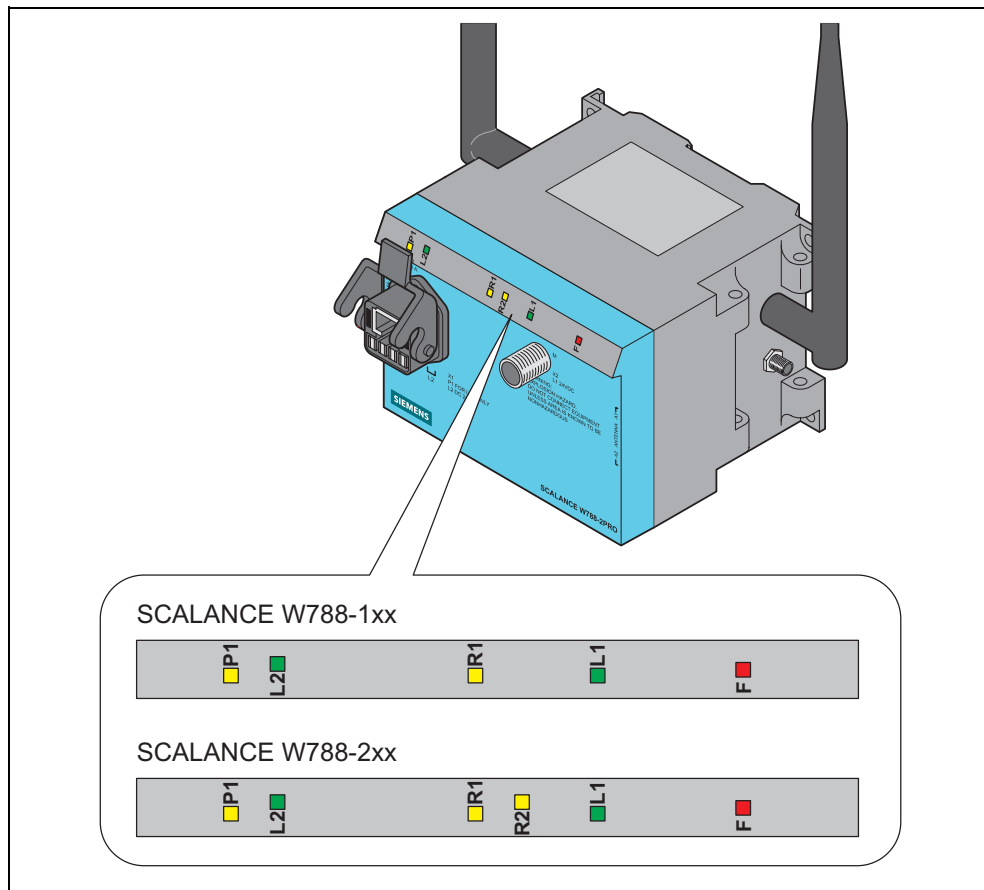


Figure 2-1 The LEDs of the SCALANCE W78x

The LEDs have the following significance:

LED	Color	Meaning
P1	Yellow	Data transfer over the Ethernet interface (traffic).
	Green	There is a connection over the Ethernet interface. (Link)
	Yellow flashing	PRESET-PLUG detected.
	Yellow/green	PRESET function completed successfully.
	Green flashing	"Flashing" enabled over PST.
L2	Green	Power supply over the hybrid connector X1 (PoE or energy contacts).
R1	Yellow	Data transfer over the first WLAN interface.
	Green	<i>Access Point Mode:</i> The WLAN interface is initialized and ready for operation. <i>Client Mode:</i> There is a connection over the first WLAN interface.
	Green flashing	<i>Access Point Mode:</i> The channels are scanned. <i>Client Mode:</i> The client is searching for a connection to an access point or ad hoc network.
	Green flashing quickly	<i>Access Point Mode:</i> With 802.11h the channel is scanned for one minute for primary users before the channel can be used for data traffic. <i>Client Mode:</i> The client waits for the adopt MAC address due to the setting <Auto Find Adopt MAC> and is connected to no access point.
	Yellow flashing	PRESET-PLUG detected.
	Green 3x fast, 1x long flashing	<i>Client Mode:</i> The client waits for the adopt MAC address due to the setting <Auto Find Adopt MAC> and is connected to an access point.
	Yellow/green	PRESET function completed successfully.

LED	Color	Meaning
R2	Yellow	<i>Access Point Mode:</i> Data transfer over the second WLAN interface. <i>Client Mode:</i> The LED is always off because the 2nd interface is not available in client mode.
	Green	<i>Access Point Mode:</i> The WLAN interface is initialized and ready for operation. <i>Client Mode:</i> The LED is always off because the 2nd interface is not available in client mode.
	Green flashing	<i>Access Point Mode:</i> The channels are scanned. <i>Client Mode:</i> The LED is always off because the 2nd interface is not available in client mode.

LED	Color	Meaning
	Green flashing quickly	<i>Access Point Mode:</i> With 802.11h the channel is scanned for one minute for primary users before the channel can be used for data traffic. <i>Client Mode:</i> The LED is always off because the 2nd interface is not available in client mode.
	Yellow flashing	PRESET-PLUG detected.
	Yellow/green	PRESET function completed successfully.
L1	Green	Power supply over the M12 connector (X2).
F	Red	An error occurred during operation with the SCALANCE W78x.

Note

If the LED for the WLAN interface is not green when the device starts up, although it is activated, the interface is not ready for operation (interface not initialized).

The main reason for this is usually that during commissioning of the SCALANCE W78x products, a waiting time of up to 15 minutes can occur when the ambient temperature is below zero. The device is ready for operation at the specified ambient temperature as soon as the LED for the WLAN interface is lit green.

Configuration Information on the C-PLUG

The C-PLUG is used to transfer the configuration of the old device to the new device when a device is replaced. When the new device starts up with the C-PLUG, it then continues automatically with exactly the same configuration as the old device. One exception to this can be the IP configuration if it is set over DHCP and the DHCP server has not been reconfigured accordingly.

Reconfiguration is necessary if you use WDS or redundancy and use the MAC addresses and not the sysNames. These functions are then based on the MAC address that inevitably changes if a device is replaced.

Note

As soon as the device is started with a C-PLUG inserted, the SCALANCE W starts up with the configuration data on the C-PLUG.

Replacing the C-PLUG

Follow the steps below to replace a C-PLUG in a SCALANCE W78x:

- 1 Turn off the power to the device.
- 2 Remove the old SCALANCE W78x from its mounting and open the sealing screw on the rear with a coin or broad screwdriver.
- 3 Remove the C-PLUG.
- 4 Open the sealing screw of the new device in the same way and insert the C-PLUG of the old device.
- 5 Replace the sealing screws of both devices.

If a new C-PLUG is inserted in a SCALANCE W78x, the configuration stored locally on the SCALANCE W78x is saved to the C-PLUG. If an incorrect C-PLUG (for example from another device or a damaged plug) is inserted, the SCALANCE W78x signals an error with the red LED. The user then has the choice of either removing the C-PLUG again or selecting the option to reformat the C-PLUG and use it.

Note

It is necessary that the configuration on the C-PLUG was generated with a firmware version \leq the firmware version on the destination device.

Example: A C-PLUG with version V3.0 cannot be used for a SCALANCE W78x with firmware version V2.4.

Reset Button

The reset button is on the rear of the device directly beside the C-PLUG receptacle and has several functions:

- **Restarting the device.**

To restart the device, press the Reset button.

- **Loading new firmware**

(Only if the normal procedure for loading firmware with Load & Save (see Section. 6.2.10) does not work). This can, for example, occur if there was a power down during the normal firmware update.

Follow the steps below to load new firmware:

1. Turn off the power to the device.
 2. Now press the Reset button and reconnect the power to the device while holding down the button.
 3. Hold down the button until the red fault LED (F) starts to flash after approximately 2 seconds.
 4. Now release the button. The bootloader waits in this state for a new firmware file that you can download by FTP.
 5. Assign an IP address with the Primary Setup Tool.
 6. Connect a PC to the SCALANCE W78x over the Ethernet interface.
 7. Then enter the command "ftp <ip address>" in a DOS box or use a different FTP client. The new firmware should be located in the same folder as the DOS box.
 8. For the login and password, enter "siemens". You can now transfer the new firmware with the "put <firmware>" command.
 9. Once the firmware has been transferred completely to the device, the device is restarted automatically.
- **Restoring the default parameters (factory default)**
Caution: All previously made settings are lost!
First, turn off the power to the device. Now press the Reset button and reconnect the power to the device while holding down the button. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit. **Now release the button and wait until the fault LED (F) goes off again. The device then starts automatically with the default parameters.**

- **Adopting the configuration data from the PRESET PLUG.**
If the device restarts with a valid PRESET PLUG, by pressing the button briefly, the configuration data is adopted by the device.

Commissioning

3

3.1 Lightning Protection, Power Supply, and Grounding

Notes on Lightning Protection



Warning

Antennas installed outdoors must be within the area covered by a lightning protection system. Make sure that all conducting systems entering from outdoors can be protected by a lightning protection potential equalization system.

When implementing your lightning protection concept, make sure you adhere to the VDE 0182 or IEC 62305 standard.

A suitable lightning conductor is available in the range of accessories of SIMATIC NET Industrial WLAN:

Lightning Protector LP798-1PRO (order no. 6GK5798-1LP00-0AA6)



Warning

Installing this lightning protector between an antenna and a SCALANCE W788 is not adequate protection against a lightning strike. The LP798-1PRO lightning protector only works within the framework of a comprehensive lightning protection concept. If you have questions, ask a qualified specialist company.

Note

The requirements of EN61000-4-5, surge test on power supply lines are met only when a Blitzductor VT AD 24V type no. 918 402 is used

Manufacturer: DEHN+SÖHNE GmbH+Co.KG Hans Dehn Str.1 Postfach 1640 D-92306 Neumarkt, Germany

Safety extra-low voltage (SELV)



Warning

The SCALANCE W78x devices are designed for operation with safety extra-low voltage (SELV). Therefore only safety extra-low voltage (SELV) with limited power source (LPS) complying with IEC950/EN60950/VDE0805 may be connected to the power supply terminals.

The power supply unit to supply the SCALANCE W78x must comply with NEC Class 2 (voltage range 18 - 32 V, current requirement 1 A)

The device may only be supplied by a power supply unit that meets the requirements of class 2 power sources of the "National Electrical Code, table 11 (b)". If the power supply is designed redundantly (two separate power supplies), both must meet these requirements.

Exceptions:

- Power supply with PELV (according to VDE 0100-410) is also possible if the generated rated voltage does not exceed the voltage limits 25 V AC or 60 V DC.
 - Power supply by a SELV power source (according to IEC 60950) or PELV power source (according to VDE 0100-410) without limited power is also permitted if suitable fire protection measures are taken by:
 - Installation in a cabinet or suitable enclosure
 - Installation in a suitably equipped, closed room
-

Grounding

Caution

There must be no potential difference between the following parts otherwise there is a risk that the device will be destroyed:

- Ground potential of the power supply and ground potential of the antenna ground.
- Ground potential of the power supply and a grounded housing.
- Ground potential of the power supply and the ground potential of the device connected to Industrial Ethernet (for example PC, AS-300, AS-400 etc.)

Connect both grounds to the same foundation earth or use an equipotential bonding cable.

Power over Ethernet

Connecting several SCALANCE W7xx devices with PoE supply from a common PoE switch (acting as power supply) is not possible.

3.2 Assembly and Connectors

Securing the Housing

There are two ways of securing the housing:

- Use the holes in the housing to screw the device to the wall or on a horizontal surface.
- Install the SCALANCE W78x on a 90 mm long, vertically mounted piece of standard rail (S7-300). In this case, the standard rail serves as an adapter between the wall and SCALANCE W78x. If you want to install the SCALANCE W78x along with a PS791-1PRO, a 150 mm long standard rail is necessary.
- Make sure that there is suitable strain relief for the connecting cable.

Note

We recommend that you protect the device from direct sunlight with a suitable shade. This avoids unwanted heating of the device and prevents premature ageing of the device and cabling. When operating the SCALANCE W outdoors, make sure that it is installed so that it is protected from UV and that the device is not exposed to rain (installed under a roof).

Note

The minimum distance to fluorescent lamps should be 0.5 m. For cabinet installation, we recommend that you do not install relays on the same or on directly neighboring mounting rails.

Connectors for the Power Supply and for Ethernet

The SCALANCE W78x is attached to Ethernet via a hybrid socket on the front of the housing (position **A** in Figure 3.1). This port also has contacts for the operating voltage.

Note

If you do not use the hybrid socket, this must be covered with a protective cap, otherwise IP 65 protection is lost. A suitable protective cap is available as an accessory (order no. 6ES7194-1JB10-0XA0). If you do not use the M12 connector, the supplied protective cap must also be fitted to retain the IP65 degree of protection.

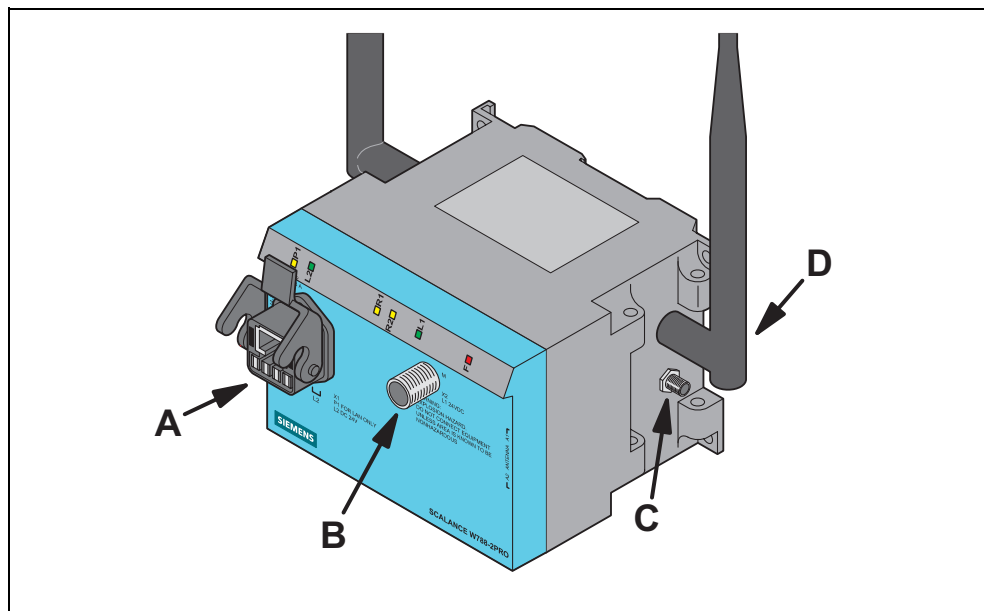


Figure 3-1 Connectors of the SCALANCE W78x

As an alternative or in addition to this, you can also use the M12 plug for the power supply (position **B** in Figure 3.1).

You can fit additional antennas to the sides of the SCALANCE W788-2PRO and SCALANCE W788-2RR with an antenna cable (position **C** in Figure 3.1). If you install the SCALANCE W78x in a cabinet, the antenna (position **D** in Figure 3.1) must be unscrewed due to the restricted communication. In this case, the connection is over detached antennas in store outside the cabinet. On the front panel, there is also an identifier for the antenna connectors. The A connectors are on the right-hand side and B connectors B on the left-hand side.

SIMATIC NET offers the IWLAN FRNC antenna extension cable for the connection between the SCALANCE W78x and detached antenna. To avoid violating the approvals, only antennas released for this product can be used.

Note

The distance between a pair of antennas for the first and second WLAN interface must be at least **0.5 m**.

3.3 Cabling for Power Supply and Ethernet

3.3.1 General Notes

Suitable Cables

The following cable variants are available to connect a SCALANCE W78x to the power supply and to Ethernet:

- IE hybrid cable 2 x 2 + 4 x 0.34 (order no. 6XV1870-2J)

The two data wire pairs are separately shielded. This cable is particularly suitable for assembly with the IE IP 67 hybrid connector.

- IE FC TP standard cable 4 x 2 GP (order no. 6XV1870-2E)
IE FC TP flexible cable 4 x 2 GP (order no. 6XV1870-2H)

In these cable types, two wires are twisted. All four pairs of wires are inside a common shield.

- 2 x 2 IE cable, the optional power supply (18 - 32 V DC) is over M12 connectors.

Cable Selection and Interference Exposure

A decisive factor in the selection of a cable type is the electromagnetic interference to which the current lines between the power supply and the FC RJ-45 modular outlet are subjected. Due to the separate shielding of the data wires, such interference has less effect on the data transmission on a hybrid cable than on TP standard cable or TP flexible cable.

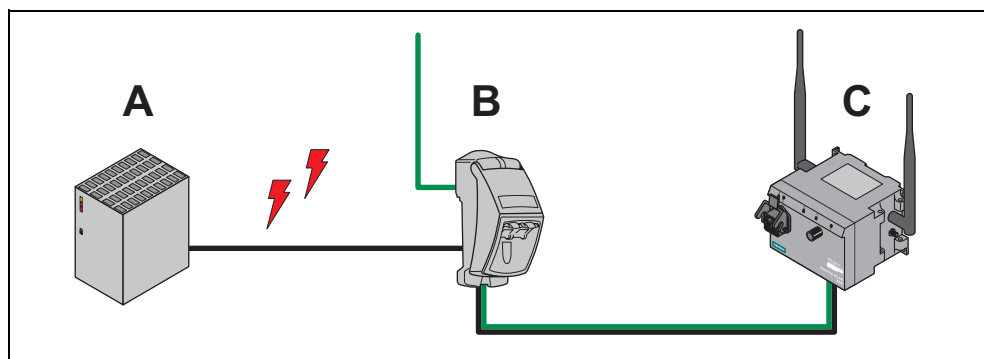


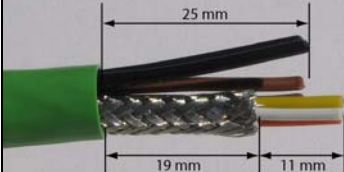

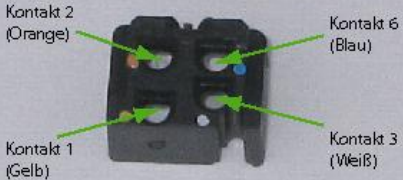


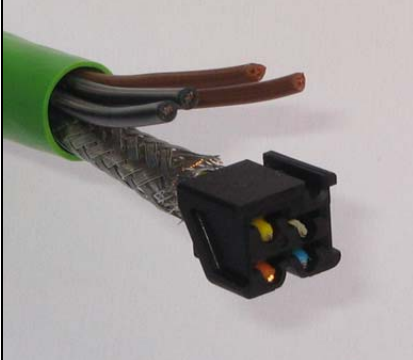
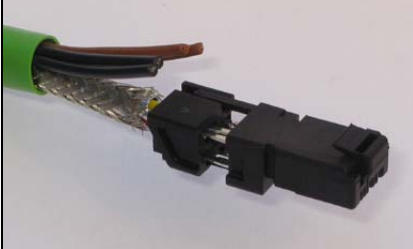
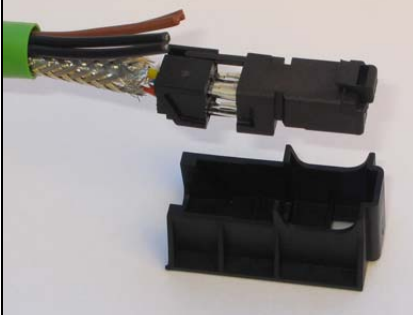
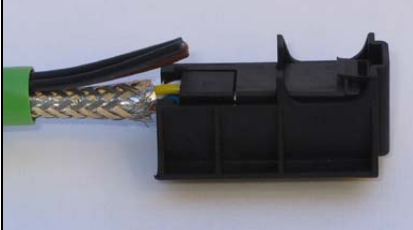
Figure 3-2 Cabling a SCALANCE W7xx with Electromagnetic Interference between the Power Supply and Modular Outlet

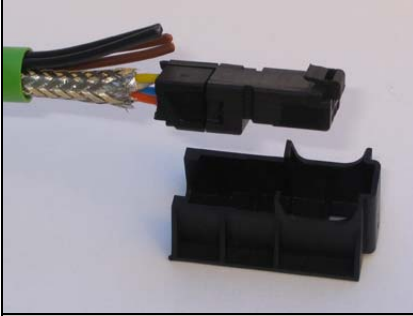

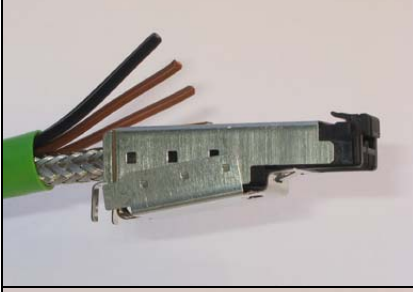
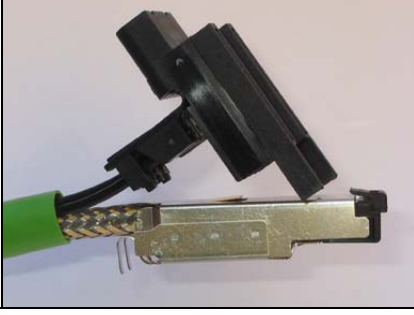
- A Power supply
- B FC RJ-45 modular outlet with power insert
- C SCALANCE W78x

3.3.2 Assembling an IE Hybrid Cable 2 x 2 + 4 x 0.34 with an IE IP 67 Hybrid Connector

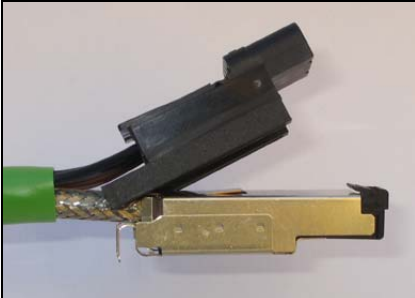



	<p>Remove the two inner shells of the universal sealing ring to adapt it to the diameter of the hybrid cable.</p>
	<p>Push the bushing, washer, adapted universal sealing ring and the housing over the cable jacket.</p>
	<p>Remove the following lengths of cable jacket and shield braid:</p> <ul style="list-style-type: none"> • 25 mm for the power leads. • 30 mm jacket for the data leads (shorten the braid by 11 mm). <p>Cut off the filler at the height of the cable jacket.</p>
	<p>Arrange the data leads according to the color codes on the splice element. The following table shows the assignment of the data leads.</p>
	<p>Contact and color assignment of the splice element.</p>

Wire color code (standard)	White	Blue	Yellow	Orange
Connector color code (Siemens IE)	White	Blue	Yellow	Orange
Siemens IE FC RJ-45 socket (reference)	3	6	1	2



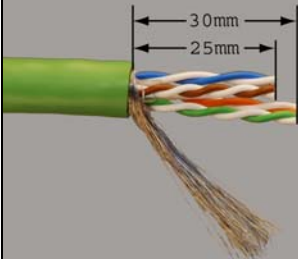

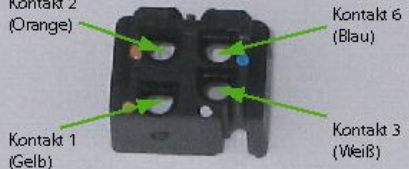
	Insert the all the data leads at the same time into the splice element is far as they will go.
	Close the splice element and RJ-45 data module until they lock together.
	Insert the data module and the splice element into the supplied IDC assembly tool.
	Press the data module and the IDC assembly tool together to establish the installation piercing connection.

	Remove the assembled data module from the IDC assembly tool.
	Position the top shield plate and press it over the cable shield.
	Position the lower shield plate and press it and the upper shield plate together until they lock together with an audible "click".
	Arrange the power leads and insert them as far as they will go into the hinge elements of the isolation body. The following table shows the assignment of the power leads.

Wire color code (standard)	Brown	Brown	Black	Black
	24 V	24 V	Ground	Ground
Power supply insert module	1	2	3	4

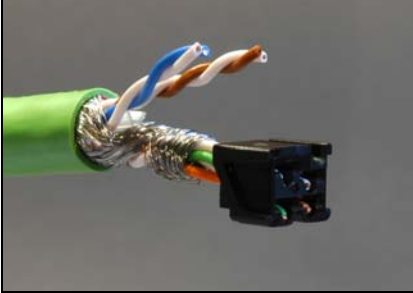
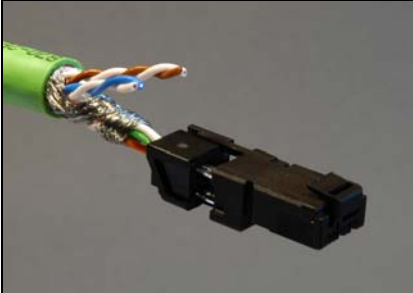
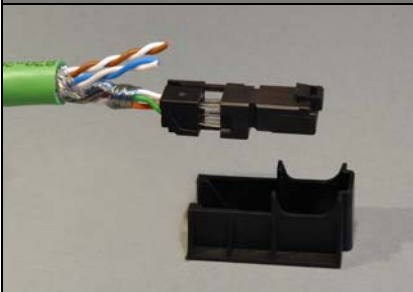
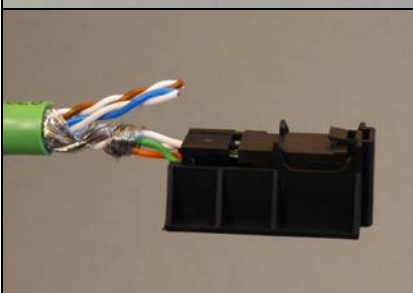
	<p>Press each individual hinge element together with the integrated IDC contact.</p> <p>Recommendation: Use a small slotted screwdriver (max. 3.5 mm) as a lever.</p>
	
	<p>Push the housing over the assembled data module and the insulator body until they lock together (there should be an audible click).</p>
	<p>Tighten the cable gland. We recommend an open ring key with a size of 21 mm.</p>

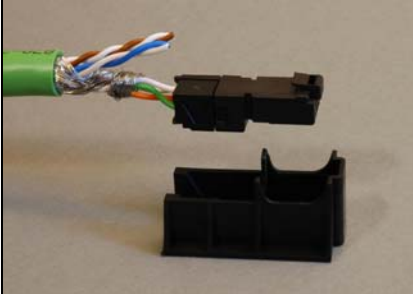
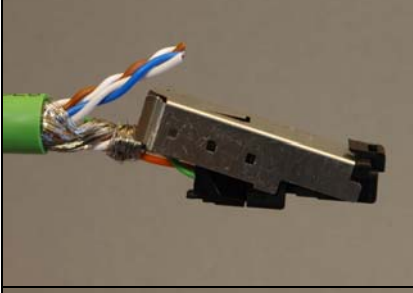
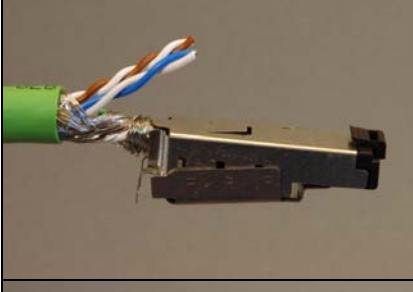
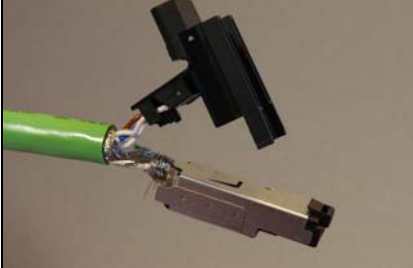
3.3.3 Assembling an IE FC TP Standard Cable 4 x 2 GP or IE FC TP Flexible Cable 4 x 2 GP with an IE IP 67 Hybrid Connector

	<p>Remove the two inner shells of the universal sealing ring to adapt it to the diameter of the hybrid cable.</p>
	<p>Push the bushing, washer, adapted universal sealing ring and the housing over the cable jacket.</p>
	<p>Remove the following lengths of cable jacket and shield braid:</p> <ul style="list-style-type: none"> • 25 mm for the power leads. • 30 mm for the data leads. <p>To achieve good shielding, the shield braid must be at least 30 mm long.</p>
	<p>Arrange the data leads according to the color codes on the splice element. The following table shows the assignment of the data leads.</p> <p>Wind the shield braid around the data leads. As a result, the shielding of the cable has contact to the shield plate of the splice element that will be fitted later.</p>
	<p>Contact and color assignment of the splice element.</p>

Color Coding of the Standard Cable	White / Orange *	Orange	White / Green *	Green
Connector color code (Siemens IE)	White	Blue	Yellow	Orange
Siemens IE FC RJ-45 socket (reference)	3	6	1	2

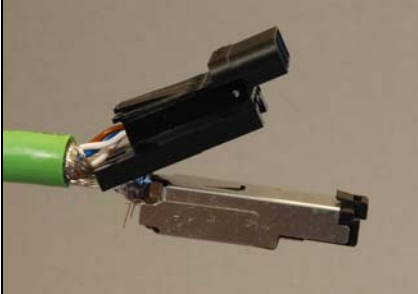
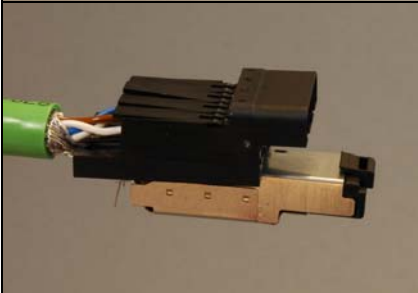


* White wire of the particular pair.

	Insert the all the data leads at the same time into the splice element is far as they will go.
	Close the splice element and RJ-45 data module until they lock together.
	Insert the data module and the splice element into the supplied IDC assembly tool.
	Press the data module and the IDC assembly tool together to establish the installation piercing connection.

	Remove the assembled data module from the IDC assembly tool.
	Position the top shield plate and press it over the cable shield.
	Position the lower shield plate and press it and the upper shield plate together until they lock together with an audible "click".
	Arrange the power leads and insert them as far as they will go into the hinge elements of the isolation body. The following table shows the assignment of the power leads.

Wire color code (standard)	White / Blue *	Blue	White brown *	Brown
	24 V	24 V	Ground	Ground
Power supply insert module	1	2	3	4

* White wire of the particular pair.

	<p>Press each individual hinge element together with the integrated IDC contact.</p> <p>Recommendation: Use a small slotted screwdriver (max. 3.5 mm) as a lever.</p>
	
	<p>Push the housing over the assembled data module and the insulator body until they lock together (there should be an audible click).</p>
	<p>Tighten the cable gland. We recommend an open ring key with a size of 21 mm.</p>

3.3.4 Pinout of the M12 Connector

	X2 Socket
PIN 1	24 V DC
PIN 2	--
PIN 3	Ground
PIN 4	--

3.4 Commissioning with the PRESET PLUG

How It Works

With the PRESET PLUG, it is simple to assign a configuration to WLAN devices such as access points, ECMs or IWLAN/PB links. You transfer an existing configuration to any number of other devices using the PRESET PLUG. This procedure is particularly useful when commissioning a lot of WLAN clients with the same parameter settings because you do not need to set parameters for each client manually.

Note

To avoid duplicating IP addresses, the IP parameters are not changed but are retained when you use the PRESET PLUG.

If the PRESET PLUG is inserted, the WLAN interface of the device is deactivated. WLAN operation with a PRESET PLUG insert it is not possible.

Note

With a version V3.0 AP or older, it is not possible to create a PRESET-PLUG for the IWLAN/PB-Link version V1.1. Please use a version V2.4 AP or older. If you update the IWLAN/PB Link to firmware V1.2, the configuration is available again on a PRESET PLUG (created with V3.1).

Creating a Configuration with a new PRESET-PLUG

Follow the steps below to save a configuration on a PRESET PLUG:

1. Insert the PRESET PLUG in the C-PLUG slot of a powered-down device with the required configuration and then turn on the device.
2. Start Web Based Management and select the *System > C-PLUG* menu.
3. In the *Modify C-PLUG* list box, select the *Create PRESET-PLUG* entry.

C-PLUG Status and Information

Device Boot From: C-PLUG (OK)

C-PLUG State: ACCEPTED

C-PLUG Device Group: SCALANCE W-700

C-PLUG Device Type: SCALANCE W788-2PRO

Configuration Revision: 1

File System: SIMATIC NET FS

File System Size (Bytes): 4194304 Usage (Bytes): 20019

C-PLUG Info String: 6GK5788-2ST00-2AA6 SCALANCE W788-2PRO

Modify C-PLUG: Create PRESET-PLUG Modify

PRESET-PLUG for: SCALANCE W744-1PRO (ECM)

SCALANCE W744-1PRO (ECM)
 SCALANCE W746-1PRO (ECM with IP Mapping)
 SCALANCE W747-1RR (ECM with iPCF)
 SCALANCE W788-1PRO (AP)
 SCALANCE W788-2PRO (Dual AP)
 SCALANCE W788-1RR (AP with iPCF)
 SCALANCE W788-2RR (Dual AP with iPCF)
 IWLAN/PB LINK

Refresh

4. In the *PRESET PLUG for* box, specify the device for which you want to create the PRESET PLUG.

Note

A PRESET PLUG for configuring a SCALANCE W78x in Access Point mode must be created with a SCALANCE W78x because a SCALANCE W74x does not have all the configuration settings required for the W78x.

5. Click on the *Modify* button to transfer the configuration of the device to the PRESET PLUG.
6. Turn the device off and remove the PRESET PLUG.

Changing a used PRESET PLUG

1. Insert the PRESET PLUG in the C-PLUG slot of a powered-down SCALANCE W7xx and then turn on the device. The *P1* and *R1* LEDs flash yellow to signal that the PRESET PLUG was detected.
2. Start Web Based Management, there you will see the current settings of the PRESET PLUG. Make the required changes to the configuration.
3. In the *Modify C-PLUG* list box, select the *Create PRESET-PLUG* entry.
4. In the *PRESET PLUG for* box, specify the device for which you want to create the PRESET PLUG.
5. Click on the *Modify* button to transfer the configuration of the device to the PRESET PLUG.
6. Turn the device off and remove the PRESET PLUG.

Using the PRESET PLUG to commission a device

Note

To work correctly, the PRESET PLUG must have a content that matches the target device.

1. Insert the PRESET PLUG in the C-PLUG slot of the device to which you want to assign a configuration.
2. Turn on the power to the device. The LEDs *P1* and *R1* (and *R2* on a SCALANCE W7xx with two wireless interfaces) flash yellow to signal that the PRESET PLUG was detected.
3. Press the reset button beside the C-PLUG briefly to save the settings of the PRESET PLUG on the device.
4. When all the data has been transferred from the PRESET PLUG to the device, the LEDs stop flashing and are permanently lit.
5. Turn the device off and remove the PRESET PLUG.

Note

The next time the device starts up, it uses the settings from the PRESET PLUG and the previous IP configuration.

Configuring the IP Address with the Primary Setup Tool

4

4.1 Introduction

Primary Setup Tool on CD and the Internet

The Primary Setup Tool is on the CD that ships with the SCALANCE W78x.

The Primary Setup Tool is also available from Siemens Automation and Drives Service & Support on the Internet under entry ID 19440762. You will find this entry under the following URL:

<http://support.automation.siemens.com/WW/view/en/19440762>

Note

On the CD and on the Internet, you will find the latest version of the Primary Setup Tool (at the time of release of this document, Version 3.1). Make sure that you use the version V3.1 or higher for the SCALANCE W78x.

Operating Systems Supported

The Primary Setup Tool can be installed and used with the following operating systems:

- Windows XP Professional
- Windows 2000 Professional SP2

DLC Protocol

The Primary Setup Tool uses the DLC protocol for communication with the modules. Depending on the operating system you are using, you must work through the following steps before you can use the DLC protocol:

- **Windows XP Professional**
The DLC protocol is not supplied with Windows XP and must be installed and activated separately.
- **Windows 2000 Professional SP2**
The DLC protocol is supplied with Windows 2000 but must be added to the active protocols.

Note

The sections on installing the DLC protocol are relevant only for older firmware versions < V2.3.

4.2 Installation of the DLC Protocol in Windows XP Professional

Extracting the Archive File

The files for installing the DLC protocol are in the self-extracting ZIP archive *pst_install.exe*. Follow the steps below to extract the files from the archive:

1. Double-click on the file name *pst_install.exe* in the Windows Explorer or start the program using the Windows menu command *Start > Run*.
2. In the dialog box of the extraction program, select the folder into which you want to extract the files and click on the *Extract* button.

Installation

Follow the steps below to install the DLC protocol on your computer:

1. Double-click on the *setup.exe* file.
2. In the *Choose Setup Language* dialog, select the language you want to use.
3. Click on the *Next* button in the first dialog.
4. In the next dialog, select the folder in which you want to install the program and click on the *Next* button to confirm your selection.
5. Close the last dialog of the installation program by clicking on the *Finish* button.

4.3 Installation of the DLC Protocol in Windows 2000 Professional SP2

Follow the steps below to install the DLC protocol on your computer:

1. Select the menu command *Start > Settings > Control Panel > Network and Dial-Up Connections*.
2. Select the connection to your Ethernet communications module.
3. Right-click to open the context menu and select *Properties*.
4. Click on the *Install...* button in the *General* tab.
5. In the *Select Network Component Type* dialog, select the entry *Protocol* and click the *Add...* button.
6. In the *Network Protocols* window, select the entry *DLC Protocol* and confirm by clicking *OK*.
7. Close the properties dialog by clicking the *OK* button.

4.4 Installing the Primary Setup Tool

Procedure

Follow the steps below to install the Primary Setup Tool on your computer:

1. Double-click on the file name *setup.exe* in the Windows Explorer or start the program using the Windows menu command *Start > Run*.
2. In the *Choose Setup Language* dialog box, select the language in which you want to run the installation.
3. The first dialog box of the Installation Wizard opens. Click on the *Next* button.
4. The dialog box for selecting the installation folder opens. Click on the *Next* button if you want to accept the default *C:\Program Files\Siemens\Primary Setup Tool*. If you want to use a different folder, you can open a dialog box to select the folder by clicking the *Browse* button.

Start the installation by clicking the *Next* button.

5. If the DLC protocol is not installed on your computer, the *Information* dialog opens referring you to the *ReadMe file*. Confirm the dialog with *OK* and install the DLC protocol later as described in the *ReadMe file*.
6. A final dialog box informs you that the installation was successful. Click on the *Finish* button to close this dialog box.

After installation of PST V3.1, start the tool with *Start > SIMATIC > Primary Setup Tool*.

4.5 Working with the Primary Setup Tool

Selecting the Language

After starting the Primary Setup Tool, a dialog opens in which you select the language for the program. You can also set the language in the *Settings > Language* menu.

Selecting the Network Adapter

If there is more than one network adapter in your computer, you can open the *Settings > Network Adapter* menu and specify which adapter is used by the Primary Setup Tool. This menu displays a maximum of four network adapters.

Browsing the Network

Before you assign IP addresses with the PST, you must first locate the configurable devices in the network. Start this search with the steps outlined below:

- Select the *Network > Browse* menu command.
- Press the *F5* key.
- Click on the magnifier icon in the toolbar below the menu bar.

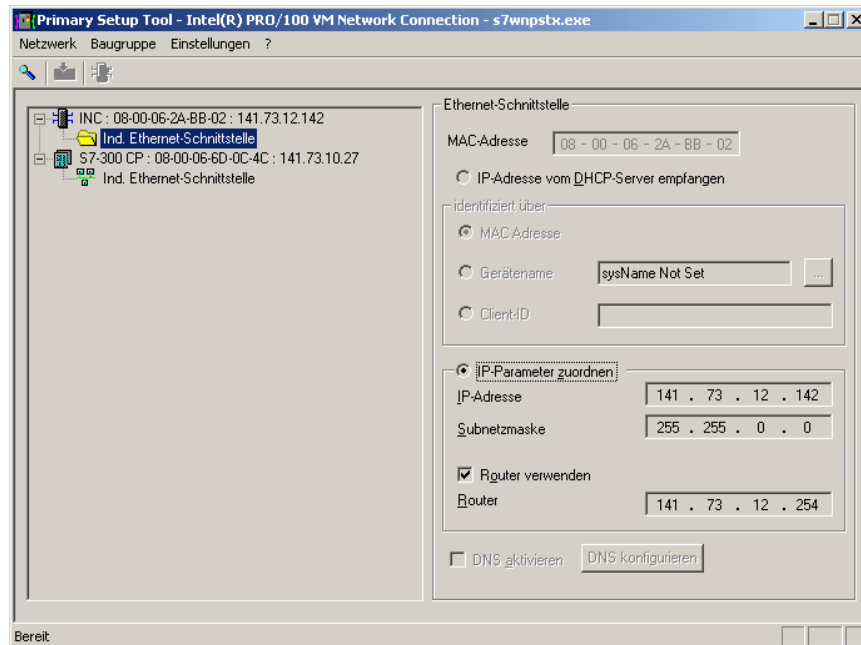
While the Primary Setup Tool browses the network, the *Browse Network* dialog is displayed with a progress bar. On completion of the search, the Primary Setup Tool displays a list with all the devices it has found in the left-hand pane.

Configuring a Module

If you click an entry in the list, the Primary Setup Tool displays information on the selected device in the right-hand pane.

Follow the steps below to configure a device:

1. Click on the plus symbol in front of the device symbol or double-click on the device symbol to display all interfaces of the device.
2. Click on the interface you want to configure. The Primary Setup Tool displays the input dialog for the configuration data in the right-hand pane of the program window. Depending on the selected settings, some text boxes or check boxes may be disabled. The *MAC address* box is always disabled because this address is a property of the device that cannot be modified. Moreover, the *Client-ID* and *DNS* parameters are not supported by the SCALANCE W7xx.



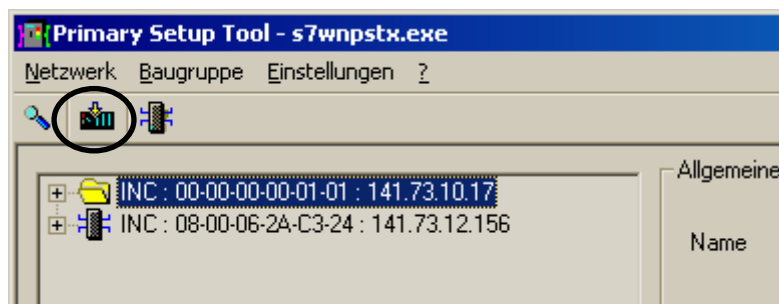
3. Decide how the device will obtain its IP address:
 - Dynamically from a DHCP server:
Select the *Obtain IP address from DHCP server* option button.
 - Manual assignment by the user:
Select the *Assign IP parameters* option button.

4. Make the following entries if you have decided to assign the IP address manually:
 - Enter the IP address for the device in the *IP Address* box. In each part of the address separated by the periods, you can enter a number between 0 and 255; the program does not accept any other numbers.
 - Enter the subnet mask in the *Subnet Mask* box.
 - If necessary, select the *Use router* check box and enter the IP address of the router in the text box. Router information is necessary if the computer on which you are creating the configuration is not in the same subnet as the device to be configured.

Downloading Configuration Data to the Module

Follow the steps below to transfer the configuration data to the device:

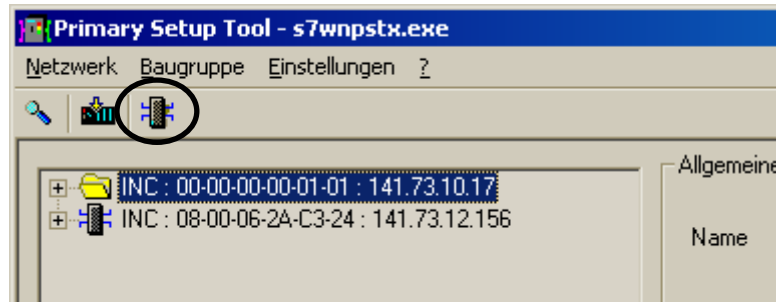
1. Select the module you want to configure in the left pane of the program window. As long as an interface is selected and the input dialog for the configuration data is displayed, no download of the configuration data is possible.
2. Start the download by following the steps outlined below:
 - Select the *Module > Download* menu command.
 - Click on the second button from the left in the toolbar.



Starting Web Based Management

INCs (Industrial Network Components) such as a SCALANCE W7xx include Web Based Management. Select the device you want to configure with Web Based Management and follow the steps below to start Web Based Management:

- Select the menu command *Module -> Start INC Browser*.
- Click on the third icon from the left in the toolbar (module with four blue wires).



If the *Module > Start INC Browser* and the module icon are disabled, there is no Web Based Management for the selected module.

Removing a Module

You can remove a module from the list in the left-hand pane of the program window by selecting the *Module > Remove Module* menu command. Using this menu command has no effect on the existence of a module in the network; if you browse the network again, all modules are displayed again.

4.5.1 Primary Setup Tool via the Command Line

Syntax

You can also use the Primary Setup Tool from the command line of a DOS prompt. The syntax is as follows; optional parameters are shown in square brackets:

`s7wnpstx MAC address -DHCP[=client ID]`

`s7wnpstx MAC address -RESET`

`s7wnpstx MAC address IP address subnet mask [router address]`

`s7wnpstx -NAME=station name [index network adapter][INC]`

The following table explains the parameters:

Command	Description	Comment
<i>MAC address</i>	The MAC address of the module to be configured.	
-DHCP	Specifies that the IP address is obtained from a DHCP server.	
<i>client ID</i>	A unique identifier for the device. If this parameter is not specified, the Primary Setup Tool uses the MAC address as the ID.	Optional.
-RESET	Sets the IP address to 0.0.0.0 .	
<i>IP address</i>	The new IP address of the module to be configured.	
<i>subnet mask</i>	The new subnet mask of the module to be configured.	
<i>Router address</i>	The new IP address of the default router.	Optional.
-NAME	Parameter for setting the station name.	
<i>station name</i>	The station name assigned to the module. Maximum length 255 characters (letters, numbers, slash, hyphen, and underscore).	
<i>Index network adapter</i>	The index of the network adapter. The default is "0".	Optional.
INC	Identifier for a network component.	Optional.

Configuration Using the Wizards of Web Based Management

5

5.1 Introduction

Principle of Web Based Management

The SCALANCE W78x has an integrated HTTP server for Web Based Management. If the SCALANCE W78x is accessed by an Internet browser, it returns HTML pages to the client computer depending on user input.

Users enter the configuration data in the HTML pages sent by the SCALANCE W78x. The SCALANCE W78x evaluates this information and generates response pages dynamically.

The great advantage of this method is that apart from a Web browser, no special software is required on the client.

Requirements for Web Based Management

Once you have assigned an IP address with the Primary Setup Tool, you can continue to configure the device with Web Based Management.

To use Web Based Management, you should ideally have a wired network connection between the SCALANCE W78x and the client computer. In principle, it is possible to use Web Based Management over a wireless network, however the SCALANCE W78x can be set so that access over a wireless network is disabled.

We recommend that you use the Microsoft Internet Explorer Version 5.5 or higher or Mozilla Firefox Version 1.5 or higher.

All the pages of Web Based Management require JavaScript. Make sure that your browser settings allow this.

Since Web Based Management is HTTP-based on, you must allow access to Port 80 or Port 443 for HTTPS if you have a firewall installed.

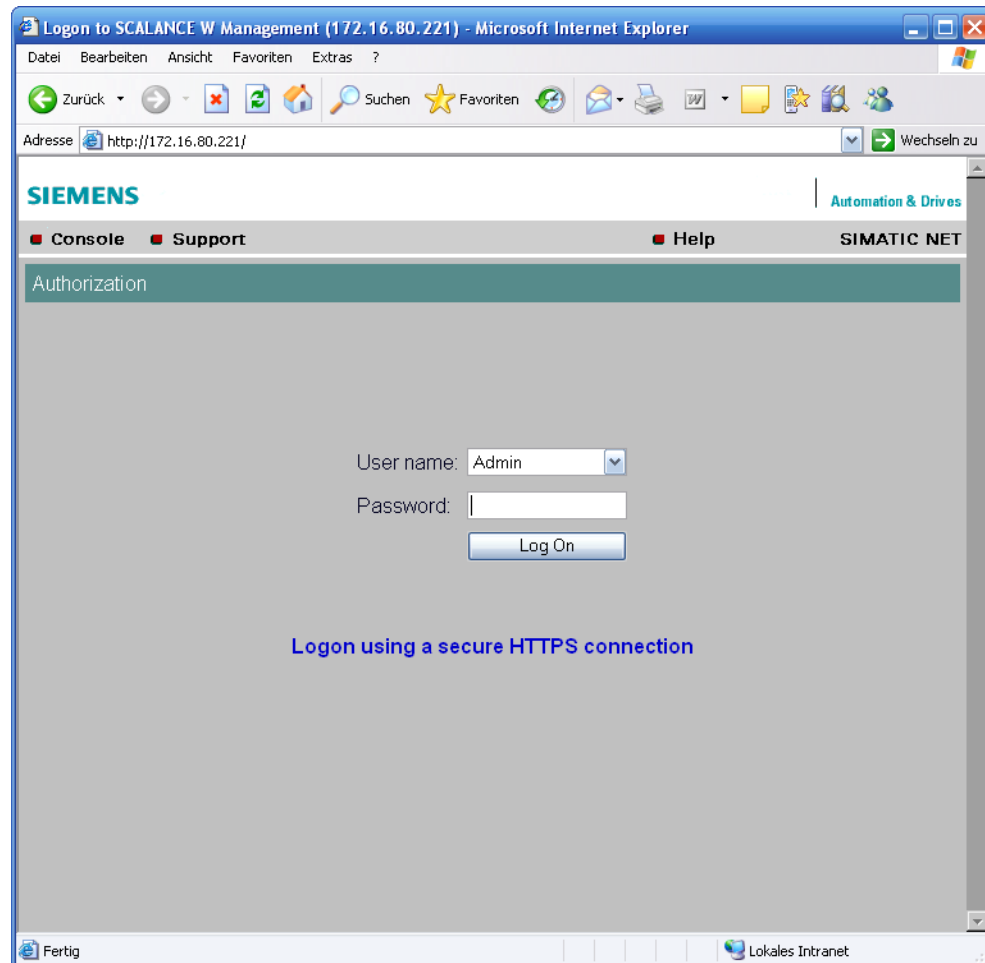
Note

The screenshots in this section were created using the Microsoft Internet Explorer version 6.0. If you use a different browser (for example Mozilla), the appearance of the menus may differ.

5.2 Starting Web Based Management and Logging On

Procedure

1. In the address box of the Web browser, enter the IP address or the URL of the SCALANCE W78x. If there is a problem-free connection to the SCALANCE W78x, the Logon dialog of Web Based Management is displayed:



2. In the "User Name" list box, select the "Admin" entry if you want to change settings of the SCALANCE W78x (read and write access). If you select the "User" entry, you only have read access to the configuration data of the SCALANCE W78x.
3. Enter your password. If you have not yet set a password, the default passwords as shipped apply: Enter *admin* if you selected "admin" as the user name or *user* if you selected "user".
4. Click on the "Log On" button to start the logon.

5.2.1 Connection over HTTPS

Description

Web Based Management also allows you to connect to the device over the secure connection of the HTTPS protocol.

Enter *https://* in the address field of the Internet browser and the *IP address* of the SCALANCE W7xx and confirm with *Enter*. The warning *Security Alert* is displayed and asks you whether you want to continue the action. Confirm with *YES*. The Login dialog of Web Based Management opens.

5.3 Selecting the Wizards

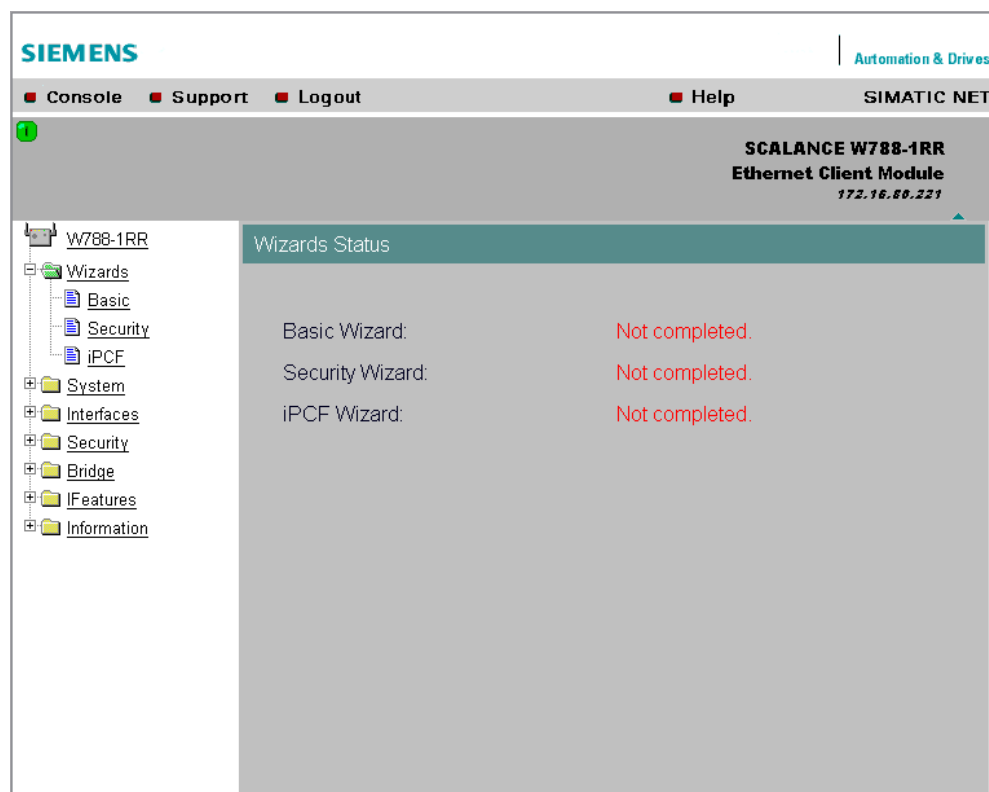
Basic Wizard, Security Wizard and iPCF-Wizard

Web Based Management provides several wizards that allow straightforward commissioning without detailed knowledge of wireless technology. A wizard consists of a series of dialogs in which you enter the basic configuration data.

There is a wizard for general settings to ensure the basic functionality of the SCALANCE W78x. The wizard for the security settings supports you when setting security-related parameters. A further wizard is available in client mode to configure the iPCF mechanism (Industrial Point Coordination Function).

Wizard Status

After selecting the "Wizards" menu on the left-hand side of the dialog, the status of the wizards is displayed. If you have worked through a wizard completely, *Done* is displayed as the status. If you have worked through all wizards, the *Wizards* entry moves to the bottom end of the menu.



The screenshot shows the Siemens Web Based Management interface. At the top, there is a navigation bar with links for Console, Support, Logout, and Help. The main header area displays "SCALANCE W788-1RR Ethernet Client Module" with the IP address "172.16.66.221". On the left side, a tree view shows the "Wizards" menu expanded, listing "Basic", "Security", and "iPCF". The main content area, titled "Wizards Status", displays the status of these wizards:

Wizard	Status
Basic Wizard:	Not completed.
Security Wizard:	Not completed.
iPCF Wizard:	Not completed.

Note

Some pages of the Wizards have a different content in access point mode and *client* mode. In this case, there is a separate description for the alternatives. You can specify the mode in the *System* menu.

5.4 Basic Wizard

5.4.1 IP Settings

Description

One of the basic steps in configuration of an Ethernet device is setting the IP address. The IP address identifies a device in the network uniquely. On this page, you enter the information for IP configuration of the SCALANCE W78x.

The screenshot shows the Siemens SCALANCE W788-1RR Ethernet Client Module web interface. The top navigation bar includes 'Console', 'Support', 'Logout', 'Help', and 'SIMATIC NET'. The main header displays 'SCALANCE W788-1RR Ethernet Client Module' with the IP address '172.16.80.221'. A left sidebar contains a tree view with folders like 'Wizards', 'System', 'Interfaces', 'Security', 'Bridge', 'IFeatures', and 'Information'. The 'Wizards' folder is expanded, showing 'Basic', 'Security', and 'iPCF'. The 'Basic' wizard is selected, leading to the 'IP Settings' page. The page contains instructions: 'Before you can setup your new device, a few settings for operation within your network must be made. This wizard will ask you for all the settings necessary.' It offers two options: 'Specified IP address' (selected) and 'DHCP server'. Below, it asks to 'Please assign a local network IP address to this device, along with the relevant netmask.' Input fields show 'IP address: 172.16.80.221' and 'Subnet mask: 255.255.255.0'. At the bottom are 'Next >>' and 'Cancel' buttons.

Specified IP Address / DHCP Server Option buttons

There are two methods of assigning IP addresses to devices: The IP address can be set as a fixed permanent address or can be obtained dynamically from a DHCP server. Select "Specified IP Address" if you do not use a DHCP server.

IP Address input box

The IP address of the SCALANCE W78x. Here, you enter an address that is unique within the network.

Subnet Mask input box

The subnet mask specifies the range of addresses within which communication can take place.

The four numbers of an IP address separated by periods are interpreted as a bit pattern. If a one is set at a bit position within the subnet mask, this means that only devices with an IP address that matches the IP address of the SCALANCE W78x Management Agent at this bit position can communicate with the SCALANCE W78x.

Example

Let us assume that the IP address of the SCALANCE W78x is set to 192.168.147.189 and the subnet mask is set to 255.255.255.0. The bit pattern for 255 is 1111 1111. This means that the bit pattern of the first number of the IP address of a communication partner must match the bit pattern of the SCALANCE W78x exactly at this point. The same applies to the second and third parts of the IP address. The IP address of a communication partner must therefore start with 192.168.147. The bit pattern of 0 is 0000 0000. This means that the bit pattern of the last part of the IP address of the partner device does not need to match the address of the SCALANCE W78x at any point; in other words, it can be any number.

5.4.2 System name

Description

The device name also identifies a network node but means more to the user than the IP address.

The screenshot shows the Siemens SCALANCE W788-1RR web interface. The top navigation bar includes 'SIEMENS', 'Automation & Drives', and links for 'Console', 'Support', 'Logout', 'Help', and 'SIMATIC NET'. The main header identifies the device as 'SCALANCE W788-1RR Ethernet Client Module' with IP address '172.16.80.221'. A left sidebar contains a tree view with folders like 'W788-1RR', 'Wizards', 'System', 'Interfaces', 'Security', 'Bridge', 'IFeatures', and 'Information'. The 'Wizards' folder is expanded, showing 'Basic', 'Security', and 'iPCF'. The 'Basic' wizard is selected, leading to the 'System Name' configuration page. The page has a title bar 'System Name' and a message: 'Check or set System Name to identify your AP in Network.' Below this, there is a label 'System name:' followed by a text input box containing 'Not set'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

System Name text box

In this box, you enter the device name for your SCALANCE W78x. This parameter corresponds to the *sysName* SNMP parameter. The device name can be up to a maximum of 255 characters long. If you also want to use this parameter for WDS or redundancy, the maximum length is 32 characters.

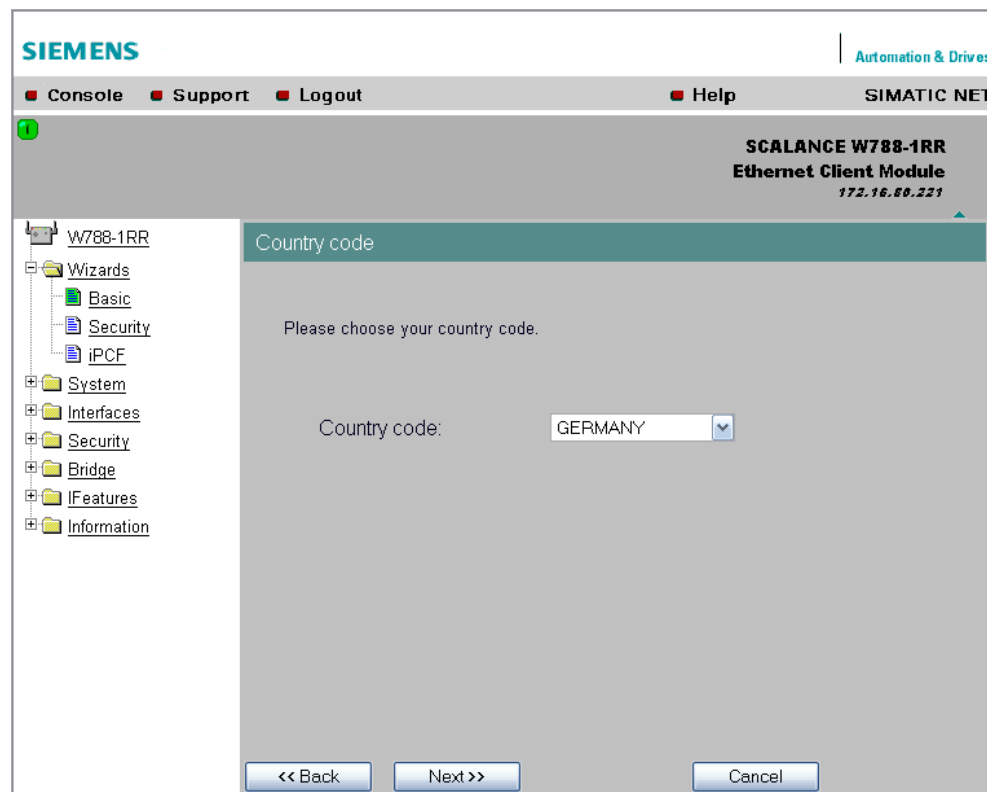
5.4.3 Country Code

Note

The correct country setting is mandatory for operation complying with the approvals. Selecting a country different from the country of use can lead to legal prosecution!

Description

Some countries have different frequency band divisions for WLAN communication. The regulations for maximum output power also differ from country to country. When you configure the SCALANCE W78x, you must specify which local regulations are relevant for your location. You do this with the *Country code* parameter.



Country code list box

In this list box, you select the country in which the SCALANCE W78x will be operated. You do not need to know the data for the specific country, the channel division and output power are set by the SCALANCE W78x according to the country you select.

5.4.4 Wireless Settings in Access Point Mode

Description

On this page, you specify the configuration of the wireless network. This includes the network name and the transmission mode. If you are configuring the SCALANCE W788-2PRO and SCALANCE W788-2RR models, this page appears a second time to allow you to configure the second wireless adapter. You can make different settings for "WLAN1" and "WLAN2".

The screenshot shows the Siemens SCALANCE W788-1RR Access Point configuration interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main title is "SCALANCE W788-1RR Access Point" with the IP address "172.16.80.221". On the left, a tree view shows the configuration structure: W788-1RR, Wizards (Basic, Security), System, Interfaces, Security, Bridge, Filters, IFeatures, and Information. The "Wireless Settings" section is active, displaying instructions: "Enter a network name (SSID) for your wireless network. Any name can be used, but the same name must be used with all other stations in the network." Below this, there are two input fields: "SSID:" with the text "Siemens Wireless Network" and "Wireless mode:" with a dropdown menu set to "2.4 GHz 54 Mbps (802.11g)". At the bottom, there are three buttons: "<< Back", "Next >>", and "Cancel".

SSID text box

Enter the name of your network in this box. The SCALANCE W78x allows all characters except the percent character for the SSID. To ensure compatibility with partner devices, you should, however, not use any characters that are peculiar to a particular language (for example special German characters ä, ö etc.). The string for SSID can be a maximum of 32 characters long.

Wireless Mode list box

Select a wireless mode that is supported by all partner devices. On the SCALANCE W788-2PRO and SCALANCE W788-2RR, it may be a practical to set a different transmission mode for each wireless adapter to allow optimum support of different clients. The effect of the *802.11.b + g* setting is that all the settings in the *Advanced G* menu are taken into account as far as possible but that compatibility with devices conforming to IEEE 802.11 b guaranteed.

5.4.5 Wireless Settings in Client Mode

Description

In the *Client* mode, there is also the check box *Connect to ANY SSID*. The other settings correspond to those of the access point mode.

The screenshot shows the Siemens SCALANCE W788-1RR Ethernet Client Module web interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main title bar identifies the device as SCALANCE W788-1RR Ethernet Client Module with IP address 172.16.88.221. A left-hand navigation tree lists various configuration categories: W788-1RR, Wizards (Basic, Security, iPCF), System, Interfaces, Security, Bridge, IFeatures, and Information. The 'Wireless Settings' page is active, displaying instructions to enter a network name (SSID) and a note that the same name must be used with all other stations. It features a 'Connect to ANY SSID' checkbox (currently unchecked), an SSID text field containing 'Siemens Wireless Network', and a 'Wireless mode' dropdown menu set to '2.4 GHz 54 Mbps (802.11g)'. At the bottom are navigation buttons: '<< Back', 'Next >>', and 'Cancel'.

Connect to ANY SSID Check Box

When this check box is selected, the client connects to the access point that allows the best possible data transfer and to which a connection is permitted based on the security settings.

5.4.6 Adopt MAC Address Settings (Client Mode only)

Assigning the MAC Address

A MAC address must be specified for the device connected to the Ethernet port of the SCALANCE W78x client before it can be reached. This MAC address is used by the client for wireless communication with the access point.

- If there is precisely one MAC address to be served downstream from the client, there are two ways of doing this:
 - Automatically, the client adopts the source MAC address of the first frame that it receives over the Ethernet interface.
 - Manual entry by the user.

These settings have no effect on communication with standard Wi-Fi devices.

- If up to eight MAC addresses need to be served downstream from the client, the following setting is available for SCALANCE W746-1PRO and SCALANCE W747-1RR:
 - Layer 2 Tunneling

This setting meets the requirements of industrial applications in which MAC address-based communication with several devices downstream from the client is required. Clients with this setting cannot connect to standard Wi-Fi devices and SCALANCE W access points with firmware V3.0 or older.

Note

The layer 2 tunneling setting is available only with the following model variants:

- SCALANCE W78x in client mode
 - SCALANCE W746-1PRO
 - SCALANCE W747-1RR
-

The SCALANCE W746-1PRO and SCALANCE W747-1RR devices can also provide access to a wireless network for several Ethernet devices (IP mapping). For an access point with MAC filtering, only one MAC address is visible to the SCALANCE W78x client, there can be no filtering according to the MAC addresses of the Ethernet devices.

MAC mode list box

Here, select how the SCALANCE W78x client obtains a MAC address. The following are possible:

Auto find 'Adopt MAC'

The SCALANCE W78x client automatically adopts the source MAC address of the first frame that it receives over the Ethernet interface.

Set 'Adopt MAC' manually

You enter the MAC address manually.

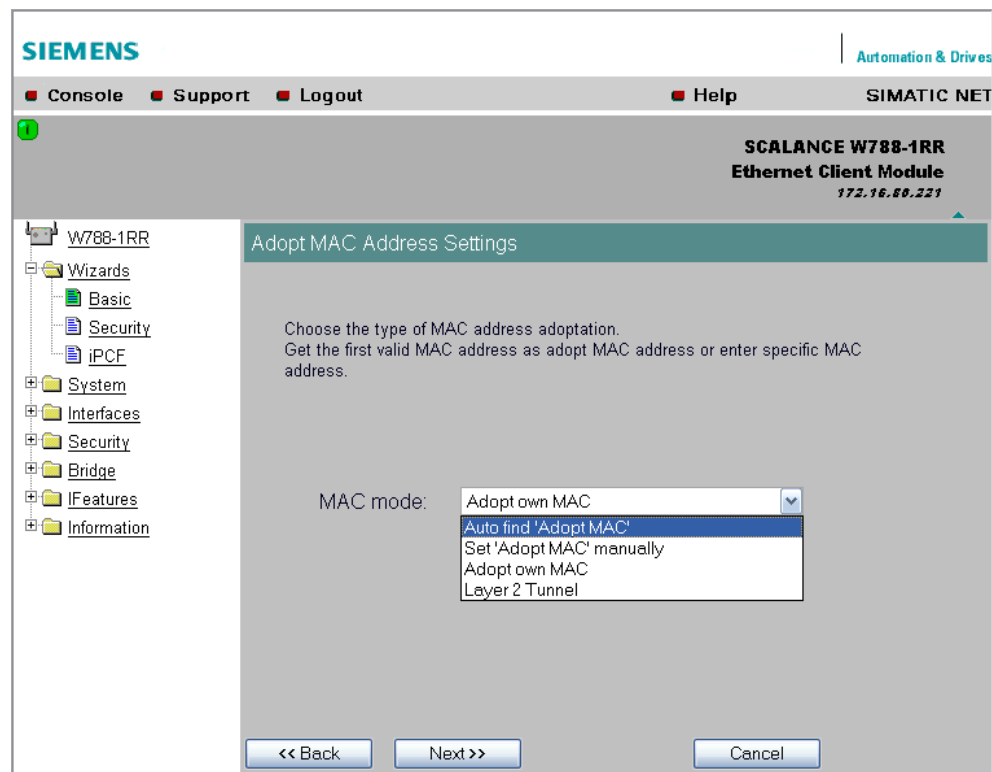
Adopt own MAC (not for SCALANCE W744-1PRO)

The SCALANCE W74x uses the MAC address of the Ethernet interface for the WLAN interface.

Layer 2 Tunneling (not for SCALANCE W744-1PRO)

SCALANCE W74x uses the MAC address of the Ethernet interface for the WLAN interface. The network is also informed of the MAC addresses connected downstream from the SCALANCE W746-1PRO or SCALANCE W747-RR.

The screenshot shows the Siemens SCALANCE W788-1RR Ethernet Client Module web interface. The top navigation bar includes 'Console', 'Support', 'Logout', 'Help', and 'SIMATIC NET'. The main header displays 'SCALANCE W788-1RR Ethernet Client Module' and the IP address '172.16.80.221'. On the left, a tree view shows the configuration structure: W788-1RR, Wizards (Basic, Security, iPCF), System, Interfaces, Security, Bridge, IFeatures, and Information. The 'Adopt MAC Address Settings' wizard is active, displaying instructions: 'Choose the type of MAC address adoption. Get the first valid MAC address as adopt MAC address or enter specific MAC address.' Below this, the 'MAC mode:' label is followed by a dropdown menu currently set to 'Adopt own MAC'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.



Adopt MAC text box

If the *Set 'Adopt MAC' manually* check box is selected, you will need to enter the MAC address of the device connected to the SCALANCE W78x client over Ethernet here.

If you do not want layer 2 communication to be handled over the SCALANCE W78x client, but only send higher IP-based frames to one or more connected devices, you can also leave the default setting *Adopt Own Mac*. In this mode, the client registers with the MAC address of its Ethernet adapter. The IP packets are broken down according to an internal table and forwarded to the connected devices.

The Adopt MAC box is hidden in the "Auto find 'Adopt MAC' " and "Layer 2 Tunneling" modes.

5.4.7 Channel Settings (only in access point mode)

Description

The SCALANCE W78x uses a specific channel within the frequency band for communication. You can either set this channel specifically or configure the SCALANCE W78x so that the channel is selected automatically. A specific channel must be set, for example, in the following situations:

- Communication suffers from interference from another device (for example microwaves) or another wireless network.
- Use of the redundancy function. In this case, two well spaced channels or two different frequency bands must be selected.
- Use of WDS. In this case, select a problem-free channel that is also used by the WDS partner.

The screenshot shows the Siemens SCALANCE W788-1RR Access Point web interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main header identifies the device as SCALANCE W788-1RR Access Point with IP address 172.16.80.221. A left sidebar contains a tree view with folders: W788-1RR, Wizards (Basic, Security), System, Interfaces, Security, Bridge, Filters, IFeatures, and Information. The main content area is titled 'Channel Settings' and contains the instruction 'Set channel for wireless interface.' Below this are three settings: 'Outdoor AP mode:' with an unchecked checkbox, 'Auto channel select:' with an unchecked checkbox, and 'Radio channel:' with a dropdown menu currently showing '6 (2437MHz)'. At the bottom of the main area are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Auto Channel Select Check Box

Select this check box if you do not have any particular requirements regarding channel selection.

Radio Channel list box

Here, you select a channel suitable for your application. You can only select from this list if the *Auto Channel Select* check box is not selected. The entries in the list box depend on the previous selection made in the *Country code* box and on the mode (IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11h).

Note

If your SCALANCE W78x has a second wireless adapter (SCALANCE W788-2PRO, SCALANCE W788-2RR), this adapter is deactivated when the device is shipped. You can use the second wireless adapter after you have selected the channels.

Notice

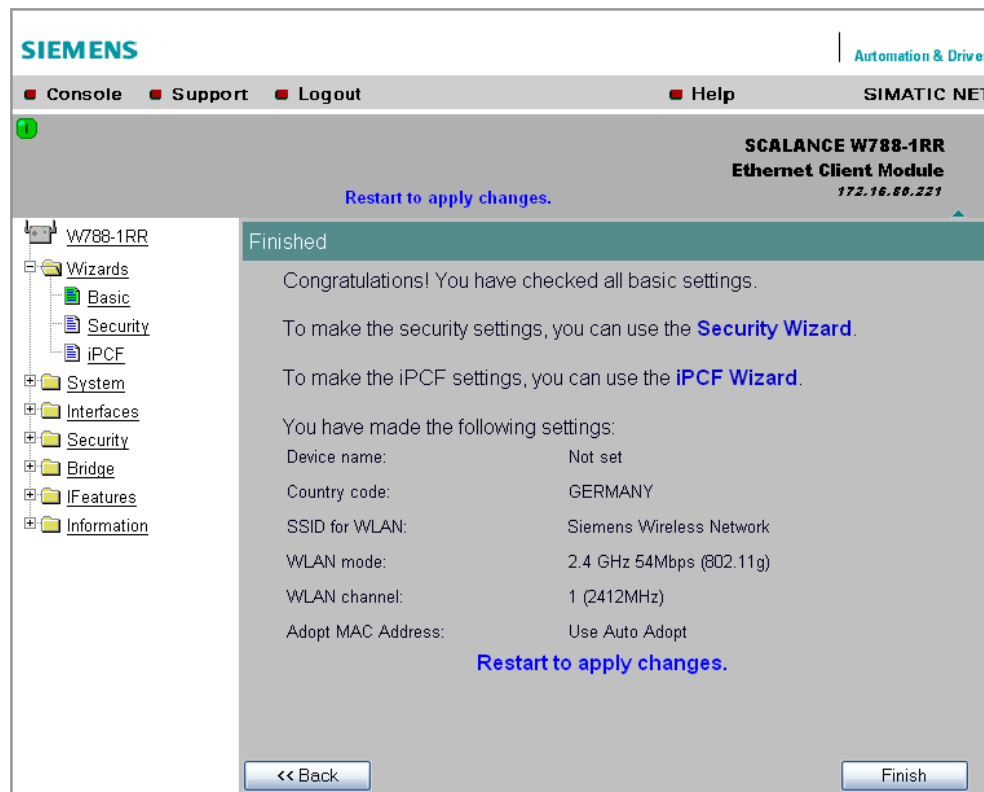
When operating a second wireless adapter, make sure that there is adequate channel spacing.

5.4.8 Finish

Description

This page displays the parameters you have selected when you have completed all the entries for the basic configuration. The setting *Adopt MAC Address* and the note on the iPCF Wizard is displayed only in client mode.

If you use a SCALANCE W788-1RR or SCALANCE W788-2RR in client mode and want to operate it in a iPCF network, you can enter the necessary settings using the *iPCF Wizard* link.



Finish button

Click this button to close the Basic Wizard and to log on again with the modified IP address. Alternatively, click on the *Security Wizard* link to change to the security settings.

5.5 Security Wizard

Introduction

With the Security Wizard, you can specify security-related parameters without detailed knowledge of security technology in wireless networks.

Note

The SCALANCE W78x can be operated even if you do not set the security parameters. Depending on the properties of your network, there is then, however, an increased risk of unauthorized access. You should therefore work through all the pages of the Security Wizard, so that you have at least basic security functions.

5.5.1 Security Settings

Password

First, set a new admin password. Enter the string twice in the text boxes of this page. The password can be up to a maximum of 31 characters long.

Until you set a password, the defaults set in the factory apply: The default password for the *admin* user is *admin*. You can use the wizards only if you log on as administrator.

The screenshot displays the Siemens SCALANCE W788-1RR web interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main header identifies the device as SCALANCE W788-1RR Ethernet Client Module with IP address 172.16.60.221. A left sidebar shows a tree view with folders for W788-1RR, Wizards (containing Basic, Security, and iPCF), System, Interfaces, Security, Bridge, IFeatures, and Information. The main content area is titled 'Security Settings' and contains the following text: 'This wizard assists you in protecting the device and your data from unauthorized access.' and 'First, set a configuration password'. Below this, there are three input fields: 'Current Admin Password:', 'Password:', and 'Confirm password:'. The 'Password:' and 'Confirm password:' fields are masked with dots. At the bottom, there are 'Next >>' and 'Cancel' buttons.

5.5.2 Security Settings for Management Interfaces

Protocols for Configuration

In this page, you specify the protocols with which you can access the configuration of the SCALANCE W78x. All protocols with a selected check box can be used for configuration. You should only select protocols that you actually use.

The protocol settings only take effect after exiting the Security Wizard and restarting. Even after selecting the *Web Based Management* entry, you still have the option of returning to earlier pages or exiting the wizard.

Specifying the Network Type for Configuration

It is easier to restrict access to a wired network than to a wireless network. Web Based Management allows access to the SCALANCE W78x for configuration to be restricted to computers linked to the SCALANCE W78x with a cable. If you require this, check the box at the bottom of the page.

The screenshot shows the Siemens SCALANCE W78x-1RR Ethernet Client Module configuration interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main title is "SCALANCE W78x-1RR Ethernet Client Module" with the IP address 172.16.88.221. The left sidebar shows a tree view with folders: W788-1RR, Wizards (Basic, Security, iPCF), System, Interfaces, Security, Bridge, IFeatures, and Information. The main content area is titled "Security Settings for Management Interfaces" and contains the following text and options:

The device's configuration may be accessed from different protocol interfaces. Here you may reduce the access rights via different protocol interfaces:

Command Line Interface (CLI) / Telnet protocol:	<input checked="" type="checkbox"/>
WEB Based Management / HTML protocol:	<input checked="" type="checkbox"/>
Simple Management Network Protocol (SNMP):	<input checked="" type="checkbox"/>

You can allow management of AP only from wired (Ethernet) interface and close management ability from wireless interface for security reason.

Allow management only from wired interface: ☐

At the bottom, there are three buttons: "<< Back", "Next >>", and "Cancel".

5.5.3 Security Settings for SNMP Protocol

Access Permissions using the SNMP Protocol

When using the SNMP protocol, you specify access permissions by means of the community string. A community string effectively combines the function of user name and password in one string; different community strings are defined for read and write permissions. More complex and more secure authentications are possible only in some SNMPv2 variants and in SNMPv3.

To preserve security, you should not use the default values *public* or *private*.

The screenshot shows the Siemens SIMATIC NET web interface. The top navigation bar includes 'Console', 'Support', 'Logout', 'Help', and 'SIMATIC NET'. The main header identifies the device as 'SCALANCE W788-1RR Ethernet Client Module' with IP address '172.16.60.221'. A left sidebar contains a tree view with folders like 'Wizards', 'System', 'Interfaces', 'Security', 'Bridge', 'IFeatures', and 'Information'. The 'Security' folder is expanded, showing 'Basic' and 'Security' sub-items. The main content area is titled 'Security Settings for SNMP Protocol'. It contains the following text: 'Set the SNMPv1 community string to protect your device from the unauthorized access over SNMPv1.' and 'You can forbid to use SNMPv1 protocol for configuration.' Below this, there is a text input field for 'Write community string:' containing the value 'private', and a checkbox for 'SNMPv1/v2 read only:' which is checked. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Write Community String text box

Here, you enter the write community string (maximum of 63 characters) for the SNMP protocol.

SNMP Read Only Check Box

If you select this check box, only read access is possible with the SNMP protocol V1 or V2c.

5.5.4 Security Settings for WLAN (Page 1, only in access point mode)

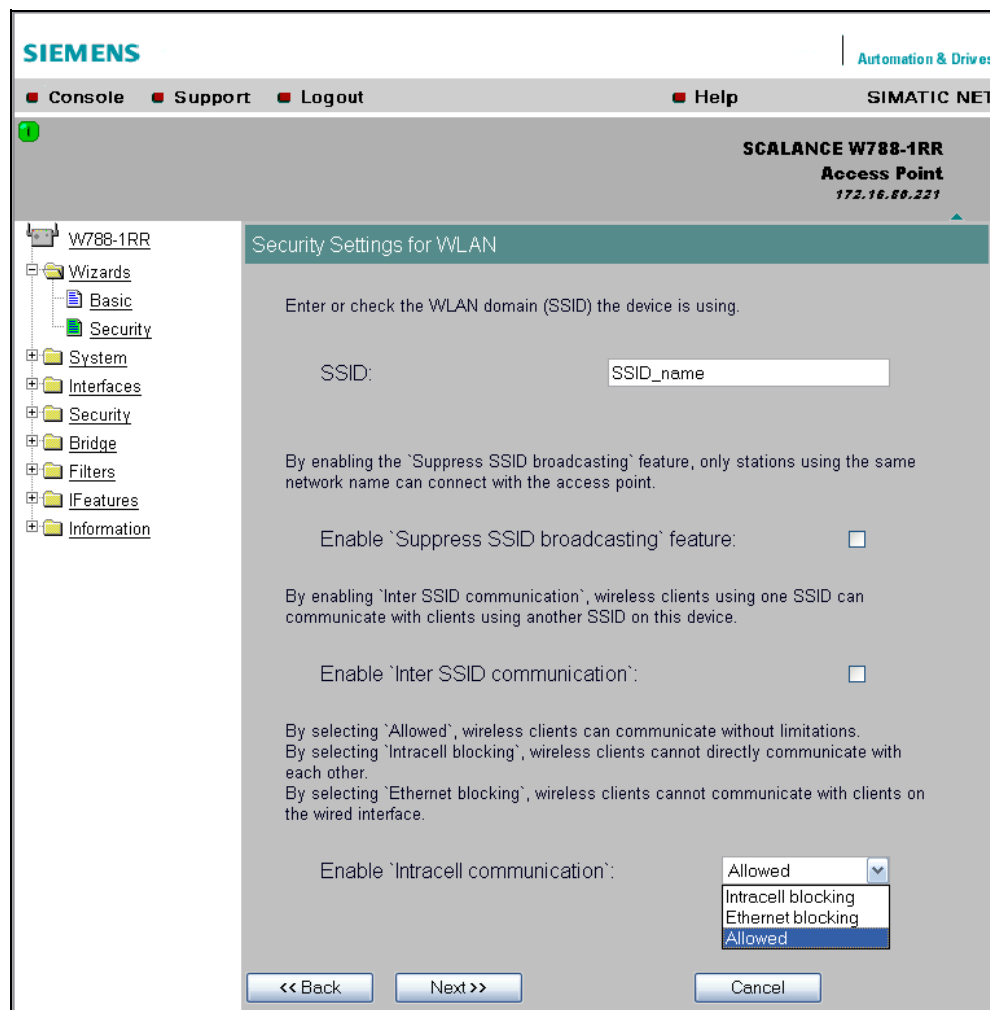
Description

On this page, you make the security settings, including, for example, the authentication and encryption. If you are configuring the SCALANCE W788-2PRO or SCALANCE W788-2RR models, these pages appear a second time to allow you to configure the second wireless adapter. You can make different settings for *WLAN1* and *WLAN2*.

Network-Specific Security Settings

On the first page of the security settings, you select settings that apply regardless of protocol-specific restrictions. The basic measures for securing a network against unauthorized access involve

- allowing only certain clients (those that have entered the network name (SSID) of the AP) to communicate with the SCALANCE W78x.
- excluding clients that communicate over wireless connections from the wired part of the network.



SSID text box

Enter the name of your network in this box (maximum of 255 characters, 32 characters if you use the redundancy function). To avoid any possible conflicts with settings for a specific locale on the computer, the name should not include any special German characters (ö, ä etc.).

Suppress SSID broadcasting check box

An entry in this check box means that the SSID is not visible for other device. As a result, only stations for which the same network name was configured as for the SCALANCE W78x can connect to the SCALANCE W78x.

Note

Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA (RADIUS) or WPA-PSK if this is not possible) provides higher security. You must also expect that certain end devices may have problems with access to a hidden SSID.

Inter SSID Communication check box

Selecting this check box allows communication between WLAN clients registered at different SSIDs of an access point.

Example 1:	A SCALANCE W788-2xx was defined with different SSIDs for each of the wireless cards.
Example 2:	A SCALANCE W788-1xx is used with multiple SSIDs.

Note

On a SCALANCE W788-2xx, the Inter SSID communication function must be enabled on both WLAN interfaces or on all VAPs to allow communication between the clients with different SSIDs.

Note

If VLANs are configured for the SSIDs, this setting can prevent communication between the SSIDs according to the VLAN rules.

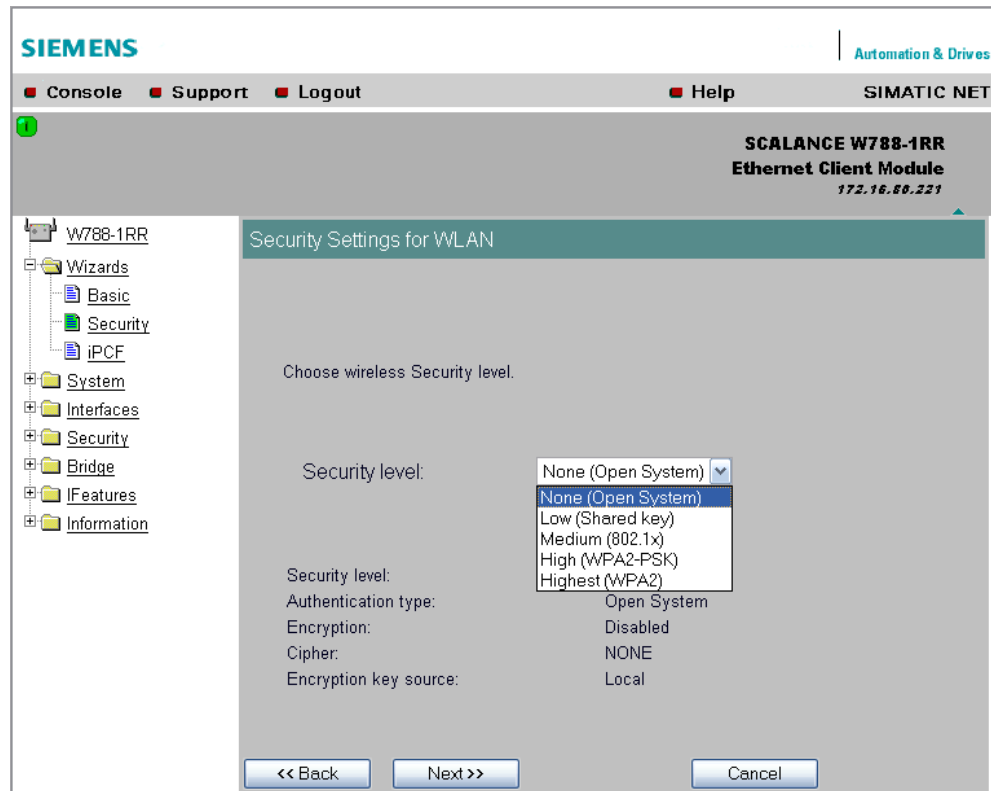
Intracell Communication list box

- *Intracell blocking*
This setting prevents WLAN client communication within an SSID.
- *Ethernet blocking*
This setting prevents WLAN client communication over the Ethernet interface of the access point.
- *Disabled*
This setting enables both WLAN client communication within an SSID as well as WLAN client communication over the Ethernet interface.

To illustrate the situation, there is an overview of the effects of the Inter SSID Communication and Intracell Communication settings below.

Settings		Possible Communication		
Inter SSID communication	Intracell Communication	within an SSID	with another SSID	to the Ethernet network
Enabled	Disabled	x	x	x
Enabled	Intracell blocking		x	x
Enabled	Ethernet blocking	x	x	
Disabled	Disabled	x		x
Disabled	Intracell blocking			x
Disabled	Ethernet blocking	x		

5.5.5 Security Settings for WLAN (Page 2)



Predefined Security Levels

Authentication and encryption are tried and tested methods for increasing security in networks. Web Based Management provides five predefined security levels that specify suitable methods.

The following table indicates what the various security levels involve.

Visible in Wizard	Level	Authentication	Encryption	Type of Encryption	Encryption key source
x	None	Open System	disabled	without	not applicable
	None	Open System	enabled as option	WEP / AES	local
x	Low	Shared Key	enabled	WEP / AES	local
x	Medium	IEEE 802.1x	enabled	WEP	Server
	High	WPA-PSK (preshared Key)	enabled	TKIP / AES	local
	Highest	WPA (Radius)	enabled	TKIP / AES	Server
x	High	WPA2-PSK (preshared Key)	enabled	TKIP / AES	local
x	Highest	WPA2 (Radius)	enabled	TKIP / AES	Server
	High	WPA-Auto-PSK (preshared Key)	enabled	TKIP / AES	local
	Highest	WPA-Auto (Radius)	enabled	TKIP / AES	Server

Authentication

Authentication basically means that some form of identification is required. Authentication therefore protects the network from unwanted access. In the *Security Level* box, you can choose between the following types of authentication:

- **None (Open System)**
There is no authentication. Encryption with a fixed (unchanging) key can be selected as an option. Based on the key length, you can choose between WEP and AES. To do this, define a key in the *Keys* menu. 5 or 13 ASCII or 10 or 26 hexadecimal characters specify a weak WEP key (40/104 bits). 16 ASCII or 32 hexadecimal characters, on the other hand, define a strong AES key (128 bits). Then select *Encryption* in the *Basic WLAN* menu.
- **Low (Shared Key)**
In Shared Key authentication, a fixed key is stored on the client and access point. This is then used for authentication and encryption. In this case, you will have to store a WEP or AES key after selecting *Low (Shared Key)*.

- Medium (IEEE 802.1x)
Port-related access check over an external RADIUS server (IEEE 802.1x). With this method, the client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. WEP is used as a weak encryption method.
- High (WPA2-PSK)
WPA2-PSK is based on the WPA2 standard, WPA authentication, however, operates without a RADIUS server. Instead of this, a key (pass phrase) is stored on every client and access point and this is used for authentication and further encryption. AES or TKIP is used as the encryption method, AES represents the standard method.
- Highest (WPA2)
WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA2 uses the additional encryption protocol CCMP that allows fast roaming in mobile ad hoc networks with its preauthentication. A client can log on in advance and several access points so that the normal authentication can be omitted. A RADIUS server is used to authenticate the client with an access point. The client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. AES or TKIP is used as the encryption method, AES represents the standard method.
- High (WPA-Auto-PSK)
Setting with which an access point can process both the *WPA-PSK* as well as *WPA2-PSK* type of authentication. This is necessary when the access point communicates with different clients, some using *WPA-PSK* and others *WPA2-PSK*. The same encryption method must be set on the clients.
- Highest (WPA-Auto)
Setting with which an access point can process both the *WPA* and *WPA2* type of authentication. This is necessary when the access point communicates with different clients, some using *WPA* and others *WPA2*. The same encryption method must be set on the clients.

Encryption

Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption in the *Encryption* check box if you have selected *Open System* for authentication in the *Basic WLAN* menu. All other security methods include both authentication and encryption. Various schemes are used for encryption:

- **WEP (Wired Equivalent Privacy)**
A weak, symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron's Code 4).
- **TKIP (Temporal Key Integrity Protocol)**
A symmetrical stream encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted packets.
- **AES (Advanced Encryption Standard)**
Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

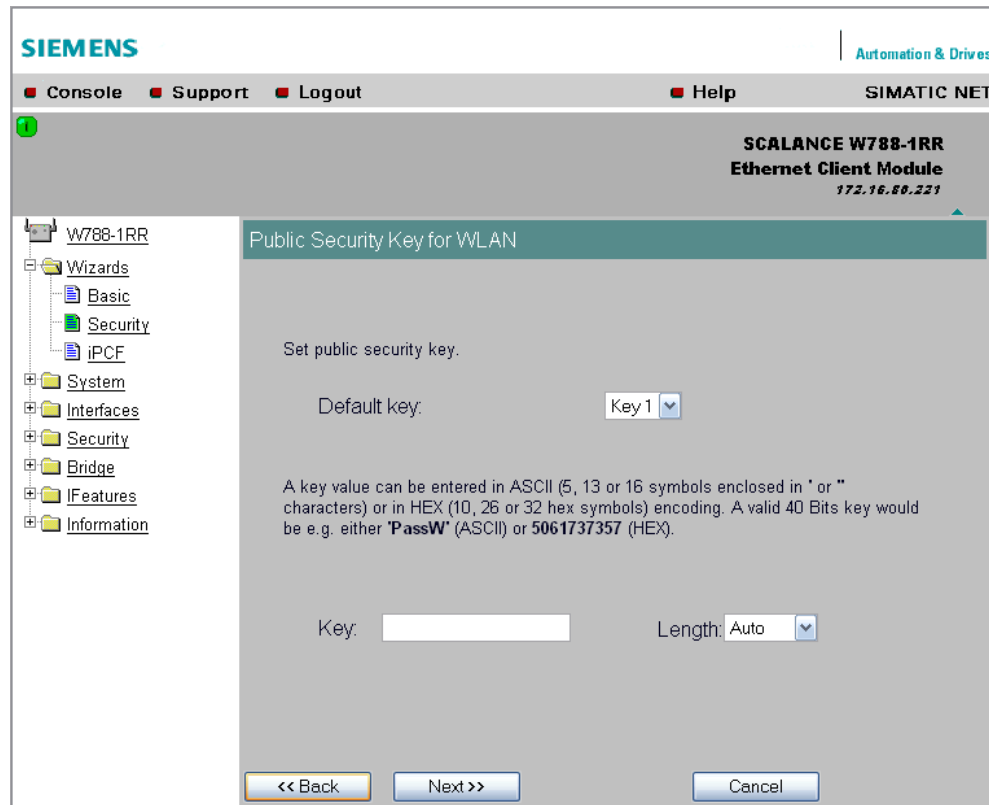
Encryption key source

The encryption key source indicates whether the key is configured locally and fixed (local) or whether it is negotiated by a higher protocol and an authentication server (server).

Security Level for WLAN list box

Select a security level that is supported by all clients. The content of the next page depends on the selected security level. If you select the security level *None*, there is no following page since neither encryption nor authentication will be used.

5.5.6 Settings for the Security Level Low



Default Key list box

Select the WEP key or AES key you want to define.

Key text box

Enter the character string for the key here. The key can be entered as ASCII characters or alternatively as hexadecimal digits (0 – F). If the key was entered in ASCII format, this is later displayed in quotes.

Length list box

Select the key length you want to use here. If the length of the string in the *Key* text box is longer or shorter than the selected key length, an error message is displayed. The following key lengths are possible:

- 40 bits WEP (5 ASCII characters or 10 hexadecimal numbers)
- 104 bits WEP (13 ASCII characters or 26 hexadecimal numbers)
- 128 bits AES (16 ASCII characters or 32 hexadecimal numbers)

With the *Auto* setting, the maximum key length is also 128 bits.

5.5.7 Settings for the Security Level Medium in Access Point Mode

Radius Authentication

Authorization lifetime (seconds):

RADIUS server	Primary	Backup
IP address:	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>
Destination port:	<input type="text" value="1812"/>	<input type="text" value="1812"/>
Shared Secret:	<input type="text"/>	<input type="text"/>
Confirm Shared Secret:	<input type="text"/>	<input type="text"/>
Maximum retransmissions:	<input type="text" value="2"/>	<input type="text" value="2"/>

Authorization Lifetime text box

Enter the period of validity of the authentication in seconds. The minimum time is 1 minute (enter *60*), the maximum time is 12 hours (enter *43200*). The default is 1 hour (3,600 seconds).

RADIUS Server Table

You can enter the data for two RADIUS servers; the information in the *Backup* column is used if the server defined in the *Primary* column is not available.

In addition to the IP address and the port, you must also specify a password (maximum 128 characters) and confirm it in a second box. In the *Maximum Retransmissions* text box, you enter the maximum number of transmission attempts. The maximum possible value is 5, the default is 2.

5.5.8 Settings for Security Level Medium in Client Mode

SIEMENS | Automation & Drives

Console Support Logout Help SIMATIC NET

SCALANCE W788-1RR
Ethernet Client Module
172.16.88.221

W788-1RR

- Wizards
 - Basic
 - Security
 - IPCF
- System
- Interfaces
- Security
- Bridge
- IFeatures
- Information

802.1x User Name and Password Configuration

The Dot1x User Name and Password are required to communicate with 802.1x Server.

Dot1x user name:

Dot1x user password:

Password confirmation:

<< Back Next >> Cancel

Dot1x user name text box

Here, enter the user name with which you want to register over the RADIUS server.

Dot1x user password text box

Here, enter the password for the above user name. The client logs on with the RADIUS server using this combination when a logon with a certificate was not possible.

Password confirmation text box

Confirm the password here.

5.5.9 Settings for the Security Level High

The screenshot shows the Siemens SCALANCE W788-1RR Ethernet Client Module web interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main header displays the device name and IP address (172.16.88.221). On the left, a tree view shows the configuration structure: W788-1RR, Wizards (Basic, Security, iPCF), System, Interfaces (Security, Bridge), IFeatures, and Information. The main content area is titled 'WPA Pass Phrase WLAN' and contains the text 'Set WPA Pass phrase.' followed by two input fields: 'Pass phrase :' and 'Pass phrase confirmation:'. At the bottom, there are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Pass phrase text box

Here, you enter a WPA2 key. The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. This initialization key must be known on both the client and the SCALANCE W78x and is entered by the user at both ends.

Pass phrase confirmation text box

Here, you confirm the entered WPA2 key.

Note

The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters). Do not use known names, words or terms that could be guessed. If a device is lost or if the key becomes known, the key should be changed on all devices to maintain security.

5.5.10 Settings for the Security Level Highest

The options you can set correspond to those of the *Medium* security level.

5.5.11 The Following Settings Were Made

Overview of the Selected Settings

This page contains an overview of the selected security settings. If you want to change a setting, you can click on the *Back* button to return to a previous page where you can enter a different value or make a different selection. In client mode, this page contains less information.

The screenshot shows the Siemens SCALANCE W788-1RR web interface. The top navigation bar includes 'Console', 'Support', 'Logout', 'Help', and 'SIMATIC NET'. The left sidebar shows a tree view with 'W788-1RR' expanded, containing 'Wizards' (Basic, Security), 'System', 'Interfaces', 'Security', 'Bridge', 'Filters', 'IFeatures', and 'Information'. The main content area is titled 'Following Settings Were Made' and lists the following settings:

CLI:	Enabled
WEB interface:	Enabled
SNMPv1:	Enabled
Management only from Ethernet:	Disabled
SNMPv1 read only:	Enabled
SSID for WLAN:	SSID_name
Suppress SSID broadcasting for WLAN:	Disabled
Inter SSID communication for WLAN:	Disabled
Intracell communication for WLAN:	Allowed
Security level for WLAN:	None

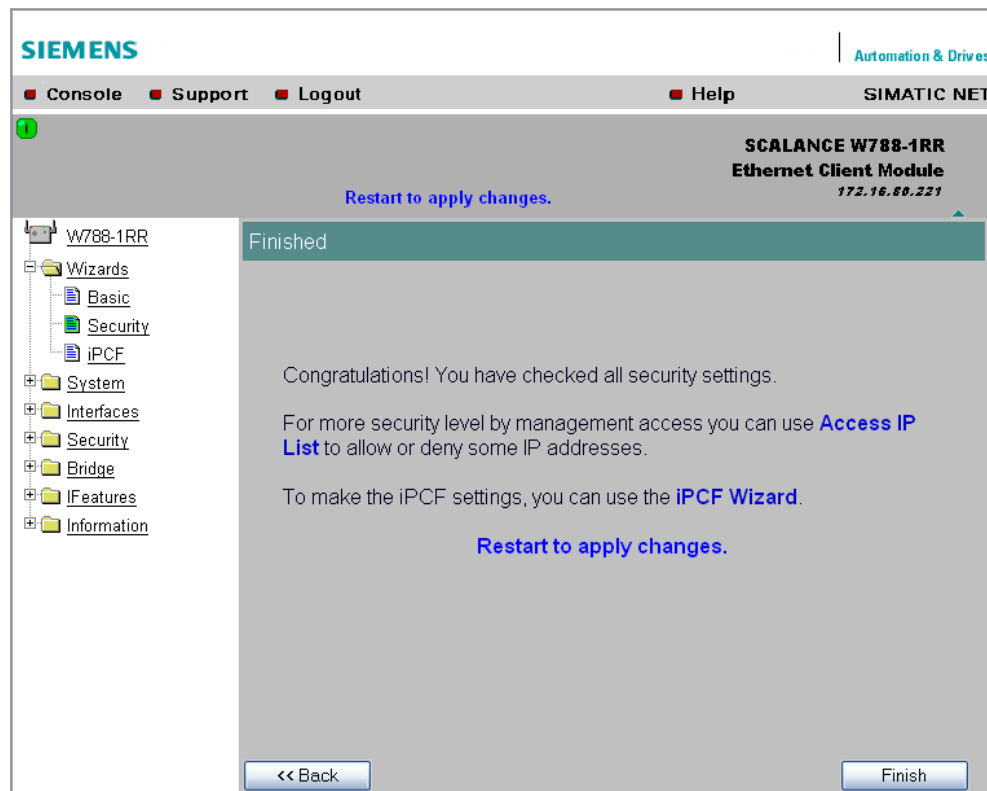
At the bottom of the page are three buttons: '<< Back', 'Next >>', and 'Cancel'.

5.5.12 Finish

Exiting the Wizard

The last page of the wizard indicates other security measures that you can take. If you still want to make final modifications, you can open the relevant pages by clicking on the texts highlighted in blue:

- IP Filter
opens the *Security > Access* page.
- Access Control List for WLAN 1 (WLAN 2)
opens the *Security > ACL* page for wireless adapter 1 or 2.
This link is available only in access point mode.
- To apply changes perform restart
opens the *System > Restart* page.



Finish button

Click the Finish button to exit the Wizard. Your settings only take effect after you have restarted (*System > Restart* menu).

5.6 iPCF Wizard

Note

The iPCF Wizard is available only in client mode of the SCALANCE W788-1RR or SCALANCE W788-2RR.

Note

The iPCF wizard also includes pages for specifying security settings. If you use iPCF, you do not therefore need to work through the Security Wizard.

5.6.1 i Point Coordination Function Settings

Channel Selection and Transmit Power

On this page, you make the setting is necessary for iPCF. The main advantage of suitable settings is that you can improve roaming times and reduce the interference affecting other systems or segments.

SIEMENS Automation & Drives

Console Support Logout Help SIMATIC NET

SCALANCE W788-1RR
Ethernet Client Module
172.16.88.221

i Point Coordination Function Settings

To optimize the scanning for further access points, you can specify channels for the client on which other access points can be found. To allow this, the Background Scan Ch. Select check box must be set and the channels of the other access point is entered in the Background Scan Channels text box. Enter the channels separated by blanks.

Background scan ch. select: ☐

Background scan channels:

In the Transmit Power list box, you can specify the output power. It may be necessary to reduce the transmit power when using antennas to avoid exceeding the maximum legal transmit power.

Transmit power:

The Diversity setting takes the best of the two antennas for the data transmission. For WLAN interface, both antennas must be connected. If only one antenna is connected, this must be selected here.
(Use "Antenna A" for IWLAN/PB Link)

Antenna mode:

Next >> Cancel

Note

When using iPCF, the following maximum data rates must be taken into account when setting the access point:

Wireless standard Max. data rate

IEEE 802.11a/h 12 Mbps

IEEE 802.11b 11 Mbps

IEEE 802.11g 12 Mbps

Background scan ch. select check box

Select this check box to restrict the number of channels on which the client searches for an access point. This results in a reduction of handover times.

Restricting the channels on which a client searches for an access point is a major factor in the reduction of handover times. To use this function, activate the *Background scan ch. select* list box and enter the channels on which access points operating in iPCF mode can actually be reached in the *Background scan channels* box.

Background scan channels text box

Here, enter the channels on which access points operating in iPCF mode can be reached by the client. If you enter more than one channel, each channel must be separated by a blank.

Transmit power list box

When using antennas, it may be necessary to reduce the transmit power to avoid exceeding the legal maximum transmit power or to restrict the visibility of the radio link. If necessary, select the required reduction in transmit power here.

A reduction of transmit power may also necessary to avoid interfering with other cells because a reduced transmit power means a reduction in the span of the cell.

Antenna Mode list box

This list box specifies the use of the antennas.

If *Diversity* is set, the SCALANCE W78x uses the **only** antenna that allows the best possible data transmission. For each WLAN interface, both antennas must be connected. Both antennas should also be of the same type and they should also illuminate approximately the same space. If an access point is operated with the diversity setting and the two antennas span different cells, this can have negative effects.

Otherwise, you must select the connected antenna. For the IWLAN-PB LINK, select *Antenna A* (see 6.3.3 section Antennas).

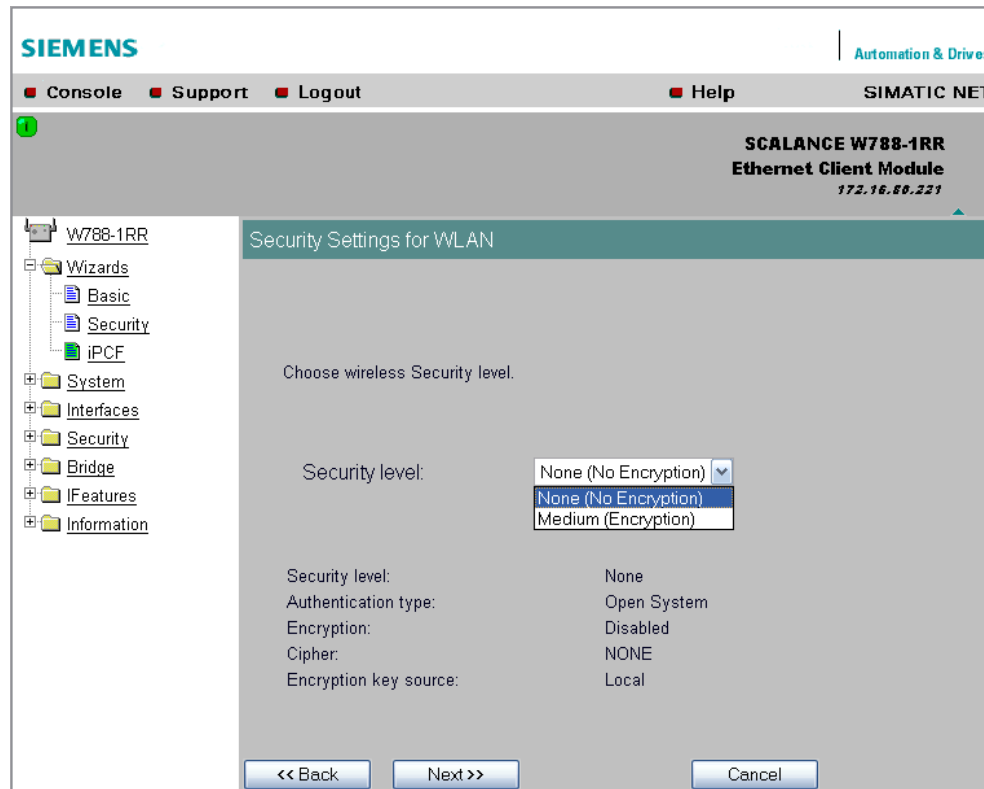
Note

If only one antenna is connected, the connected antenna must be set permanently.
The second antenna socket must also have a 50 Ω terminator fitted.

5.6.2 Security Settings for WLAN

Security Settings with iPCF

On this page, you specify the security level for the client. iPCF is a proprietary standard optimized for fast roaming and deterministic data transfer. With the current security mechanisms 802.1x and WPA, keys are negotiated using relatively time-consuming mechanisms, and they are therefore not available with iPCF.



Security level list box

Select the security level you require for your wireless network in this box. The following are possible:

- **None (no encryption)**
An open system without encryption.
- **Med (encryption)**
Static keys are used. This is the recommended setting and you should use a 128-bit AES key.

5.6.3 Public Security Key for WLAN

Specifying the Key

If you have selected the security level *Med*, you must specify the key on this page.

The screenshot shows the Siemens SCALANCE W788-1RR Ethernet Client Module configuration interface. The page title is 'Public Security Key for WLAN'. On the left is a navigation tree with folders: W788-1RR, Wizards (Basic, Security, iPCF), System, Interfaces, Security, Bridge, IFeatures, and Information. The main content area has the heading 'Set public security key.' and includes the following fields:

- Default key:** A dropdown menu currently showing 'Key 1'.
- Key:** A text input field.
- Length:** A dropdown menu currently showing 'Auto'.

At the bottom of the page are three buttons: '<< Back', 'Next >>', and 'Cancel'.

Default Key list box

Select the WEP key or AES key you want to define.

Key text box

Enter the character string for the key here. The key can be entered as ASCII characters or alternatively as hexadecimal digits (0 – F). If the key was entered in ASCII format, this is later displayed in quotes.

Length list box

Select the key length you want to use here. If the length of the string in the *Key* text box is longer than the selected key length, an error message is displayed. The following key lengths are possible:

- 40 bits (5 ASCII characters or 10 hexadecimal numbers)

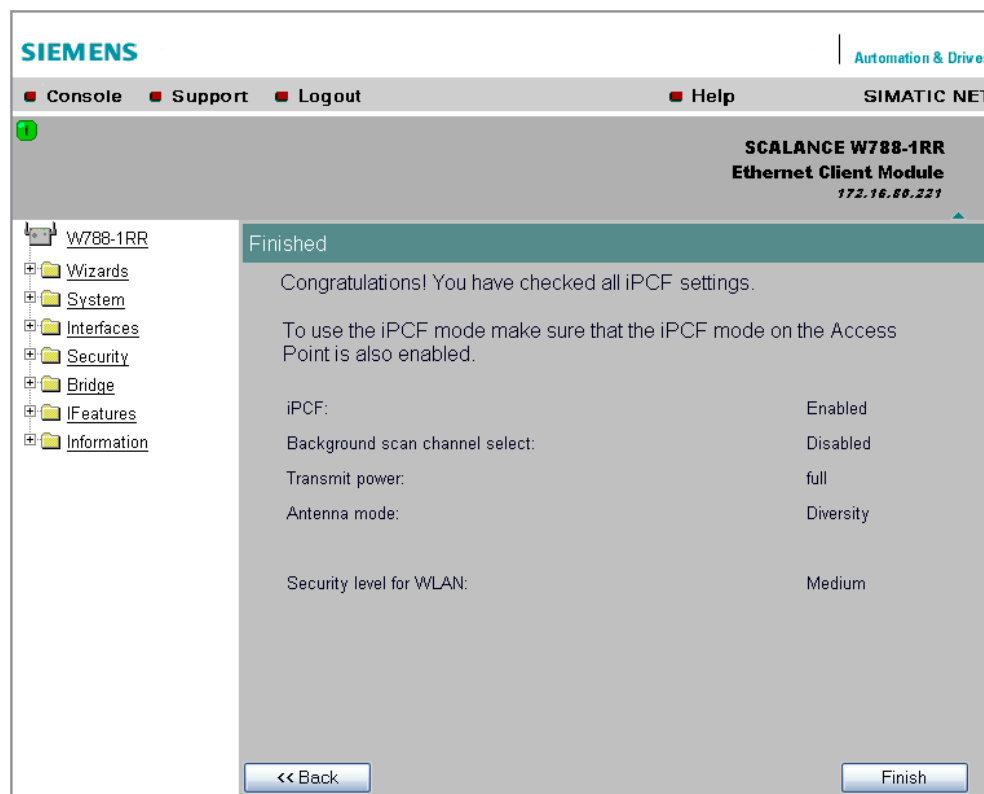
- 104 bits (13 ASCII characters or 26 hexadecimal numbers)
- 128 bits (16 ASCII characters or 32 hexadecimal numbers)

With the *Auto* setting, the maximum key length is also 128 bits.

5.6.4 Finish

Exiting the Wizard

The last page of the iPCF Wizard shows you all the settings you have made so that you can make a final check.



Finish button

Click the Finish button to exit the iPCF Wizard. Your settings only take effect after you have restarted (*System > Restart* menu).

Configuration Using Web Based Management and the Command Line Interface

6

6.1 General Information on Web Based Management and the Command Line Interface

6.1.1 Introduction

Contents of This Chapter

This chapter explains the possible settings for the SCALANCE W78x.

Web Based Management provides you with configuration options way beyond those described in the previous chapter. You will also find a detailed description of the individual elements of a page in the online help.

As an alternative, you can also configure the device using the Command Line Interface (CLI). This allows remote configuration over Telnet.

This chapter describes both configuration methods together because the menu structure of Web Based Management is the same as the structure of the CLI commands.

Note

You should only use the command line interface if you are an experienced user. Even commands that bring about fundamental changes to the configuration are normally executed without a prompt for confirmation.

Note on Login User

If you log on as user, you will only have restricted use of WEB and Telnet. Since you only have read access, some commands do not exist in Telnet and some areas cannot be selected.

Required Experience

To be able to use the information in this chapter effectively, you should have a thorough knowledge of network technology and WLANs.

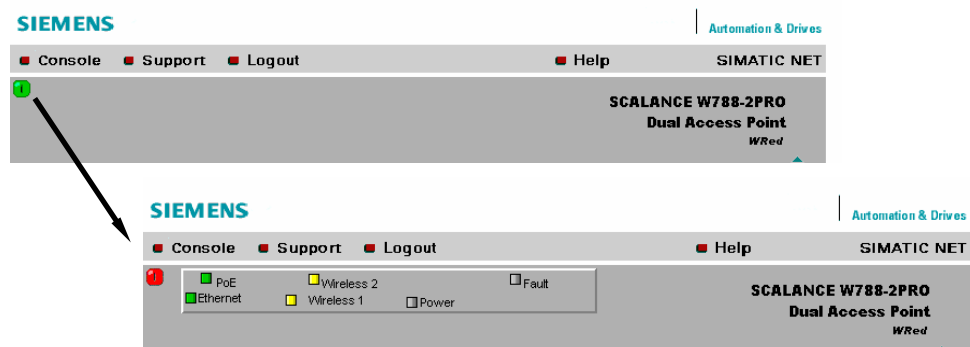
6.1.2 The LED Simulation of Web Based Management

Display of the Operating State

The SCALANCE W78x has one or more LEDs that provide information on the operating state of the device (see Chapter 2). Depending on its location, direct access to the SCALANCE W78x may not always be possible. Web Based Management therefore displays simulated LEDs.

Activating the Simulation

There is an HTML-based simulation of the LED status. Click on the green icon below the *Console* link to activate the simulation:



6.1.3 Working with Web Based Management

Navigation Bar

You will find the following links in the upper menu bar of Web Based Management (WBM):

- Console
This link opens a console window in which you can enter CLI commands.
- Support
When you click this link, you open a SIEMENS AG support page in the Internet.
- Logout
Close the current Web Based Management session by clicking on this link. The logon dialog is then displayed again.
- Help
Clicking on this link opens the online help of Web Based Management in a separate browser window.

Updating the Display with *Refresh*

Web Based Management pages that display current parameters have a *Refresh* button at the lower edge of the page. Click this button to request up-to-date information from the SCALANCE W78x.

Saving Entries with *Set Values*

Pages in which you can make configuration settings have a *Set Value* button at the lower edge. Click this button to save the configuration data you have entered on the SCALANCE W78x.

Creating Entries with *NEW*

Pages in which you can create lists have the *New* button at the lower edge. Click this button to create a new entry in the list.

Resetting a Counter with *Reset Statistics*

With this button, you can reset the relevant counters.

6.1.4 Command Line Interface (CLI)

Starting the CLI in a Windows Console

Follow the steps outlined below to start the Command Line Interface in a Windows console:

1. Open a Windows console and type in the command *telnet* followed by the IP address of the SCALANCE W78x:
`C:\>telnet <IP address>`
2. Enter your login and password.

As an alternative, you can also enter the command *telnet* followed by the IP address of the SCALANCE W78x in the *Start > Execute* menu.

Starting the CLI in Web Based Management

Click on the *Console* entry in the upper menu bar of Web Based Management. A console opens in which you can log on with your login and password. The IP address is adopted by Web Based Management.

Shortcuts for Commands

As an alternative, instead of entering full CLI commands, you can simply enter the first letter or the first few letters of the command and then press the Tab key. The Command Line Interface then displays a command starting with the letter or letters you typed in. If the command displayed is not the command you require, press the Tab key again to display the next command.

Directory Structure

Before you can enter a command in the Command Line Interface, you must first open the required menu or submenu. This section lists the commands of each menu in a separate table. The menu itself is shown above the table on a gray background. The table lists only the commands themselves.

Symbols for Representing CLI Commands

CLI commands generally have one or more parameters that are represented in the syntax description as follows:

- Mandatory parameters are shown in pointed brackets.
Example: `<IP address>`
- Optional parameters are shown in square brackets.
Example: `[E|D]`

If you omit an optional parameter, the commands output the currently set value.

- Alternative input values are separated by the pipe character. In this case, you specify *one* of the listed values as the parameter.
Example: `[E|D]`
You must enter either *E* or *D*.
- If a numeric value is required as a mandatory parameter, you can also specify a range of values:
Example: `<0 ... 255>`
You must enter a value between 0 and 255.

Cross-menu Commands

You can use the commands in the following table in any menu.

CLI \ ... >

Command	Description	Comment
/	Moves you one menu level higher.	
?	Displays the commands and submenus available in the menu.	
exit	Exits the CLI/Telnet or SSH session.	Cannot be called using the command shortcuts.
restart	Restarts the SCALANCE W78x	Cannot be called using the command shortcuts.
info	Displays information on the current menu item.	

6.2 The System Menu

6.2.1 System Information Menu Command

Mode and Locale Setting

On this page, you make several basic settings for the SCALANCE W78x, for example, the country and mode (access point or client).

For the SCALANCE W788-2RR, you can also set the *HiPath Access Point* mode.

When the mode changes from access point mode to client mode and back, all the parameters are cleared except:

- IP address
- Subnet mask
- Gateway address
- SSID (only in access point mode)
- IP address of the default router
- DHCP flag
- System name
- System location
- System contact
- Device mode
- Country code
- User and Admin IDs

Changing to the *HiPath Access Point* mode is described in section below.

The *Current system time* output box informs you about the system time. The *System up time* output box informs you about the time that has elapsed since the last *restart*.

Reading out the Country List

Enter

https:// in the address field of the Internet browser enter the *IP address* of the SCALANCE W7xx and */countrylist.log* and confirm with *Enter*.

After logging in, you then obtain the Country List with the following headers:

COUNTRY	MODE	CH	MHz	PWR(EIRP)	USAGE
---------	------	----	-----	-----------	-------

The table lists the permitted wireless modes and channels along with the corresponding channel frequencies for every possible country setting. The PWR(EIRP) rubric contains the permitted limit values for the transmit power, measured at the antenna. These values include the transmit power of the access point and the antenna gain of the antenna being used.

Note

In the version for USA/Canada, you cannot select a country. The frequency bands for these countries are already preset.

The *HiPath Access Point* Mode

Note

The *HiPath Access Point* mode is available only with the SCALANCE W788-2RR model, firmware version 2.4 or higher.

The *HiPath Access Point* mode is intended for the following situation:

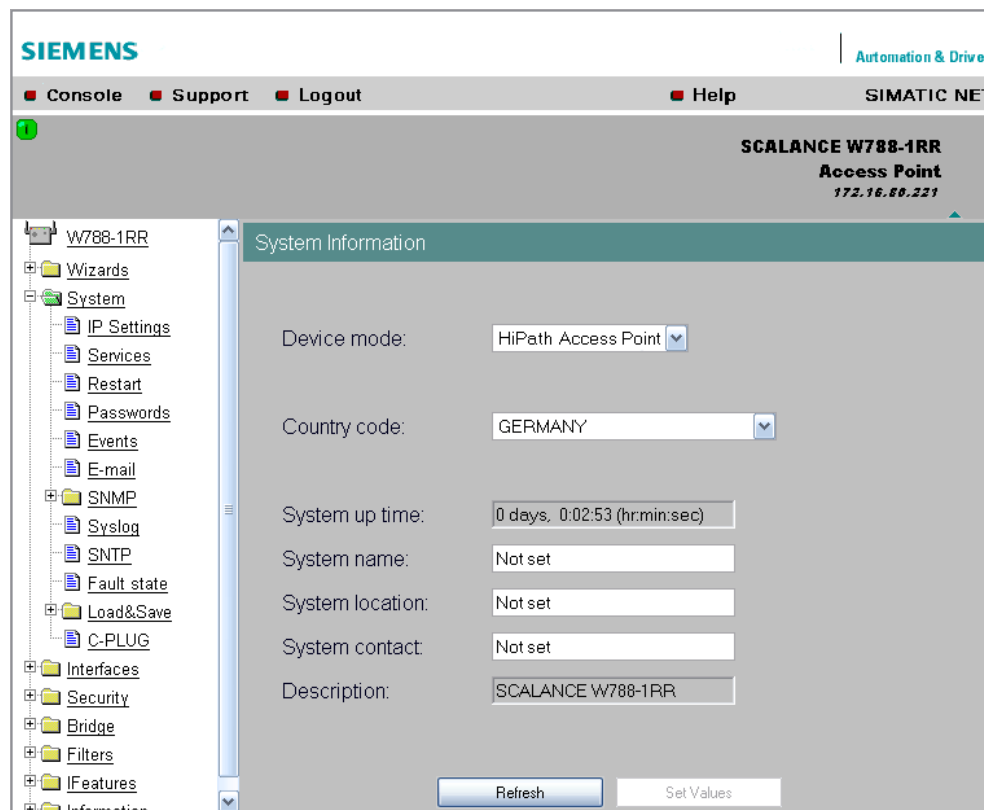
- The SCALANCE W788-2RR is an access point in a Siemens WLAN *HiPath* communications system.
 - After changing to the *HiPath Access Point* mode, the SCALANCE W788-2RR is no longer configured with the WBM or the Command Line Interface but by the *HiPath Wireless Controller* of the communications system.
-

Notice

After changing to the *HiPath Access Point* mode, the access point is returned to its default status; in other words, the configuration is lost.

If your access point was already configured and you want to use the configuration later, save it before you change over as described in Section 6.2.11, Load & Save.

Follow the steps outlined below to change the SCALANCE W788-2RR to the *HiPath Access Point* mode:



1. Connect the access point with the *HiPath Wireless Controller* and with the configuration computer over the Ethernet interface.
2. If the access point is brand new, assign an IP address.
If a DHCP server is visible, the access point is assigned an IP address automatically. Otherwise, assign the access point an IP address using the *Primary Setup Tool* (PST) (see Section 4, Configuring the IP Address with the Primary Setup Tool).
3. Connect your configuration computer with the access point in the Web browser and open Web Based Management (WBM) to the *System Information* page with *W788-2RR > System* (see Sections 5.1 and **Fehler! Verweisquelle konnte nicht gefunden werden.**).
4. In the *Device Mode* list, select *HiPath Access Point* and confirm this with *Set Values*. During configuration make sure that the SCALANCE W78x is assigned an IP address suitable for the HiPath Wireless Controller.
5. A blue message "Restart to apply changes" appears above the *System Information* WBM page.
Click on the blue message. The *Restart* window opens.
Confirm the restart by clicking on the *Restart* button.
The access point runs a restart.

6. During the restart, the access point connects to the *HiPath Wireless Controller*.
7. The access point loads the current HiPath firmware for the W788 from the *HiPath Wireless Controller* and runs a restart.
The HiPath firmware is retained in the RAM of the AP when there is a restart due to reconfiguring with the HiPath Wireless Controller.
The HiPath firmware for the SCALANCE W788 has the following name

W788-<Version>.img,
where *<Version>* stands for the current version number.

Note

After starting up with the HiPath firmware, the access point can no longer be found with the PST.

Note

Operating SCALANCE W client modules (W74x or W788 in client mode) on a HiPath access point or SCALANCE W access point in HiPath Access Point mode involves the following restrictions:

- The IP configuration of the WLAN client module (WBM page *System > IP Settings*) must not be set on to DHCP server. It may be necessary to reserve a range of IP addresses for the fixed IP settings of the WLAN client modules.
 - The *MAC Mode* parameter on the WBM page *Interfaces > WLAN* must not be set to *Adopt own MAC* (see Section 6.3.2, WLAN).
 - The WBM and Telnet of the WLAN client module can only be reached over Ethernet.
-

After loading the *HiPath* firmware, the R1 and R2 LEDs indicate the enabled antenna ports:

- **R1 lit**
The upper antenna connectors A1 and B1 are enabled (transmission standard IEEE 802.11a).
- **R2 lit**
The lower antenna connectors A2 and B2 are enabled (transmission standard IEEE 802.11b/g).

Note

In *HiPath Access Point* mode, the LEDs of the SCALANCE W788 have a different significance compared with that in the *Access Point* or *Client* mode.

Note

In *HiPath Access Point* mode, the following restrictions apply

- No use of the C-PLUG possible
- No WDS and no redundancy possible.
- No iPCF possible.
- Heavy data traffic in the cell (for example, resulting from voice) can impair the quality of the individual wireless connections (for example, S7 communication). This means that a response time cannot be defined.

The following table shows the significance of the LEDs of the HiPath access point AP2600 and the SCALANCE W788-2RR in the *HiPath Access Point* mode:

HiPath AP2600		SCALANCE W788-2RR in <i>HiPath Access Point</i> mode	
LED	Color	LED (meaning)	Color
---		P1 (Ethernet port)	Yellow/green
---		L2 (power supply Ethernet)	Green
5 GHz	Green	R1	Green
2.4 GHz	Green	R2	Green
Middle	Yellow	R1 + R2	Yellow
---		L1 (power supply M12)	Green
Middle	Red	F (fault)	Red

For the arrangement of the LEDs on the device, refer to Figure 2-1 "The LEDs of the SCALANCE W78x".

For information on the other steps in configuration, refer to the manual *HiPath Wireless Controller, Access Points and Convergence Software - User Guide*.

Exiting the HiPath Mode

If you want to return the Scalance W access point to the standard modes "Access Point" or "Client Mode", the HiPath firmware must be deleted in RAM. To do this, turn off the power to the Scalance W AP for at least 30 seconds. Following this, the AP starts up again with the SCALANCE W firmware and it is now possible to change the mode over the Web interface.

Note

Please note that if you install the SCALANCE W788 outdoors, some of the channels used indoors may not be used.

The approval of indoor and outdoor channels is country-specific. If the SCALANCE W is operated outdoors, make sure that the device is not exposed to rain (installed under a roof) and is not exposed to direct sunlight (installed with UV protection).

You will find more detailed information on HiPath Wireless, at <http://www.siemens.com/hipath>

Syntax of the Command Line Interface

CLI\SYSTEM>

Command	Description	Comment
apmode [E D H]	<p>This specifies the mode for the SCALANCE W78x:</p> <p>E Access Point</p> <p>D Client</p> <p>H HiPath Access Point (only available for SCALANCE W788-2RR)</p>	

Command	Description	Comment
country [AR AT AU BE BR BG CA CH CL CN CZ DE DK ES FI FR GB GR HK HU IE IN IS IT JP J3 KR KW LI LU NL NO PO PT RU SE SG TR US ZA]	<p>Specifies properties for specific countries. The country codes comply with ISO 3166, however the SCALANCE W78x supports only the codes listed in the left-hand column.</p> <ul style="list-style-type: none"> AR Argentina AT Austria AU Australia BE Belgium BR Brazil BG Bulgaria CA Canada CH Switzerland CL Chile CN China CZ Czech Republic DE Germany DK Denmark ES Spain FI Finland FR France GB Great Britain GR Greece HK Hong Kong HU Hungary IE Ireland IN India IS Iceland IT Italy JP Japan J3 Japan Old KR Korea KW Kuwait LI Liechtenstein LU Luxembourg NL Netherlands NO Norway PO Poland PT Portugal RU Russia SE Sweden SG Singapore TR Turkey US United States of America ZA South Africa 	This command is not available in the version for USA / Canada.

Command	Description	Comment
name [system name]	Assigns a value to the sysName MIB variable.	Maximum of 255 characters. If you want to use the name in WDS or redundancy, the maximum length is 32 characters.
location [location]	Assigns a value to the sysLocation MIB variable.	Maximum of 255 characters.
contact [name]	Assigns a value to the sysContact MIB variable.	Maximum of 255 characters.
ping [[-c N] [-s]] <IP>	For connection test to partner. -c (counter) for the number (N) of ICMPs and -s (stop) to stop ICMP frames.	Telnet only
password [admin user] [password]	Specifies a password for access to the SCALANCE W78x.	Maximum of 31 characters.

6.2.2 IP Settings Menu Command

Configuration

Here, you decide whether you will use a DHCP server or whether you want to assign a fixed IP address to the SCALANCE W78x. You can also set the IP address of a router and the default TTL. The TTL (time to live) parameter specifies the maximum number of routers passed through by a data packet before it is discarded.

Note

If you use a Radius server for authentication, this must be accessible over the management VLAN.

Syntax of the Command Line Interface

CLI\SYSTEM\IP>

Command	Description	Comment
dhcp [E D]	Enable / disable DHCP server.	
dhcptype [M N C]	Specifies how a device will be identified: M MAC address N Device name C Client ID	
clientid	Specifies a client-ID for the device.	
ip [<i>IP address</i>]	Specifies the IP address for the SCALANCE W78x.	When you enter a valid IP address, enabled DHCP is automatically disabled.
subnet [<i>subnet mask</i>]	Specifies the subnet mask.	
gateway [<i>IP address</i>]	Specifies the IP address of the router.	
tll [<i>TTL value</i>]	Sets the TTL (Time To Live) parameter.	Default value: 64

6.2.3 Services Menu Command

Configuration

Here, you select the services with which access to the SCALANCE W78x will be possible. If, for example, the *SNMP Enabled* check box is not selected, neither write nor read access is possible using the SNMP protocol (v1,v2c,v3). If the SNMP protocol is not permitted, it is not possible to send SNMP traps.

To improve security, you should only enable the services that you actually use.

Notice

Over SNMP, it is possible to disable all services and to allow read access only over SNMP. Following this, no further configuration of the SCALANCE W78x is possible.

If you *only* want to enable secure access over HTTPS when configuring the device, select the *HTTPS only* check box.

If you want to enable the response of the device to Ping signals, select the *Ping enabled* check box.

With the integrated SSH server, you have secure access to the CLI. In contrast to Telnet, the entire communication including user authentication is encrypted.

Notes on *WEB Enabled in the WEB Interface*

The check box for the *WEB Enabled* entry is selected and inactive because configuration with Web Based Management is no longer possible without the option of access with HTTP.

If you want to deactivate the option of configuration with Web Based Management, you can do this in the Security Wizard over Telnet and SNMP. Settings made using the Security Wizard only take effect after a restart on the SCALANCE W78x.

Syntax of the Command Line Interface

CLI\SYSTEM\SERVICES>

Command	Description	Comment
telnet [E D]	Enable / disable configuration of the SCALANCE W78x over Telnet.	Only WEB and SNMP
ttimeout [E D]	Enables / disables the time restriction for a Telnet session.	
ttimeout <i>[time in s]</i>	Specifies the time after which a Telnet session is closed if there is no further input.	
snmp [E D]	Enable / disable SNMP.	
mail [E D]	Enable / disable E-mail.	
web [E D]	Enable / disable configuration of the SCALANCE W78x over Web Based Management.	
https [E D]	Enable / disable access for configuring only over HTTPS.	
ping [E D]	Enable / disable response of the device to Ping.	
psu [E D]	Enable / disable access to the SCALANCE W78x with the Primary Setup Tool. If this access option is deactivated, configuration data can only be read with the Primary Setup Tool.	
ssh [E D]	Enable / disable CLI access over SSH.	

6.2.4 Restart Menu Command

Restart button

Click this button to restart the SCALANCE W78x. During a restart, the SCALANCE W78x is reinitialized, the internal firmware is reloaded, and the SCALANCE W78x runs a self-test. The entries that have been learned in the address table of the SCALANCE W78x are deleted. You can leave the browser window open while the SCALANCE W78x restarts.

Restore Memory Defaults button

Click this button to reset the configuration. The following parameters (protected defaults) are not reset:

- IP address
- Subnet mask
- Gateway address
- SSID
- IP address of the default router
- DHCP flag
- System name
- System location
- System contact
- Device mode
- Country code

There is no automatic restart. This allows you to enter data using Web Based Management before the restart. The changes take effect only after a restart.

If you are logged on as user, the *Restore Memory Defaults* button is not visible.

Restore Factory Defaults and Restart button

Click on this button to restore the factory configuration settings. The protected defaults (see above) are also reset. The C-PLUG is reinitialized and formatted if it exists. An automatic restart is triggered.

Note

By resetting all the defaults, the IP address is also lost. The SCALANCE W78x can then only be accessed using the Primary Setup Tool unless the IP address is obtained over DHCP.

If you are logged on as user, the *Restore Factory Defaults* button is not visible.

Syntax of the Command Line Interface

CLI\SYSTEM\RESTARTS>

Command	Description	Comment
restart	Restarts the SCALANCE W78x.	The <i>restart</i> command can be called from all menus, however not using the shortcut commands.
memreset	Resets the factory settings and triggers a restart (the protected settings are not deleted).	
defaults	Resets the factory settings (the protected settings are also deleted).	

6.2.5 Event Config Menu Command

System Events of the SCALANCE W78x

On this page, you specify how the SCALANCE W78x reacts to system events. You can configure the reaction of the SCALANCE W78x to the following events:

- Startup of the SCALANCE W78x
- Change in the Ethernet status Link up / Link down.
- Error in authentication.
- Changing the power supply of the SCALANCE W78x. Evaluation of this event is only useful when using a redundant power supply.
- Change in the error status

If you use the SCALANCE W78x as an Access Point, you can configure additional system events:

- IP-Alive state change (application-specific connection monitoring)
- [Link Check state change \(device-specific connection monitoring\)](#)
- Events related to bandwidth reservation iQoS
- Authentication of the client
- Detection of access points on own or an overlapping wireless channel.
- Topology changes in Rapid Spanning Tree.
- For the SCALANCE W788-1RR and SCALANCE W788-2RR models, events in conjunction with iPCF.
- Events in conjunction with the Forced Roaming on IP down function .
- Change in the WDS connection status Link up / Link down.

With the SCALANCE W788-2PRO and SCALANCE W788-2RR models, there is also the status of a redundant connection (redundant, not redundant, interrupted) as a system event.

Reaction to System Events

The following alternatives are possible:

- The SCALANCE W78x sends an E-mail.
- The SCALANCE W78x triggers an SNMP trap.
- The SCALANCE W78x writes an entry in the log file.
- The SCALANCE W78x indicates an error (the error LED lights up).

By selecting the appropriate check boxes, you specify which events trigger which reactions on the SCALANCE W78x. With the check box in the *Functions enabled* row, you enable or disable the sending of E-mails or triggering of SNMP traps.

Syntax of the Command Line Interface

For each of the four possible reactions E-mail, trap, log and fault, either *E* (Enabled, setting is enabled) or *D* (Disabled, setting is disabled) must be entered as the parameter. If, for example, an E-mail is sent when the SCALANCE W78x restarts (first parameter "CW") and an entry is made in the log table but neither a trap nor an error is generated, the following command must be entered:

```
setec CW E D E D
```

CLI\SYSTEM\EVENT>

Command	Description	Comment
setec CW <E D> <E D> <E D> <E D>	Reactions when the SCALANCE W78x restarts.	
setec LU <E D> <E D> <E D> <E D>	Reaction to the <i>Link Down</i> event on the Ethernet interface.	If the error status was triggered only due to a link down event, the error states is cleared and the error LED goes off.
setec LD <E D> <E D> <E D> <E D>	Reaction to the <i>Link Up</i> event on the Ethernet interface.	
setec AF <E D> <E D> <E D> <E D>	Reaction to a bad authentication over Web Based Management, CLI, or SNMP.	The SNMP trap <i>AuthFault</i> is sent only if there is a bad SNMP authentication.
setec PM <E D> <E D> <E D> <E D>	Reaction to a change of power supply over the M12 power connection.	
setec PE <E D> <E D> <E D> <E D>	Reaction to a change of power supply over Ethernet.	
setec FC <E D> <E D> <E D> <E D>	Reaction to a change in the error status.	
setec AP <E D> <E D> <E D> <E D>	Reaction to detection of an access point on own or an overlapping wireless channel.	This command is not available in the client mode.

Command	Description	Comment
setec MS <E D> <E D> <E D> <E D>	Reaction when the update time in iPCF mode with PNIO support cannot be kept to due to an additional client.	This command is available only on the SCALANCE W788-1RR and SCALANCE W788-2RR models but not in client mode.
setec CT <E D> <E D> <E D> <E D>	Reaction when the specified update time in iPCF mode with PNIO support cannot be kept to.	This command is available only on the SCALANCE W788-1RR and SCALANCE W788-2RR models but not in client mode.
setec IS <E D> <E D> <E D> <E D>	Reaction to a change in the connection status on a client for which the IP-alive monitoring is activated.	If the connection status changes, an event is triggered. If the connection no longer exists, the error state is triggered and the error LED is lit. This command is not available in the client mode.
setec LI <E D> <E D> <E D> <E D>	Reaction when establishing a connection monitored with the <i>Link Check</i> function.	This command is not available in the client mode.
setec IQ <E D> <E D> <E D> <E D>	Reaction to a change in the iQoS status.	This command is not available in the client mode.
setec CA <E D> <E D> <E D>	Reaction to a change in the client authentication status.	This command is not available in the client mode.
setec RD <E D> <E D> <E D> <E D>	Reaction to a change in the redundancy event status.	This command is not available in the client mode.

6.2.6 E-mail Config Menu Command

Sender and Recipient of an E-mail

Here, you specify who the SCALANCE W78x sends an E-mail to as a reaction to configured events. You can also enter a sender. This allows you to recognize which device is involved and sent the E-mail. If you do not make an entry in the *From* box, the SCALANCE W78x uses the following sender: SCALANCE_W@<IP address>

Syntax of the Command Line Interface

CLI\SYSTEM\EMAIL>

Command	Description	Comment
mail [E D]	Enable/disable the E-mail service	
email [<i>E-mail address</i>]	Specifies the address(es) to which the SCALANCE W78x sends E-mails.	Several E-mail addresses can be entered separated by semicolons.
smtp < <i>IP address</i> > [<i>:port number</i>]	Specifies the IP address and the port number of the SMTP server.	
from [<i>text for sender field</i>]	Specifies the sender of E-mails from SCALANCE W78x.	

6.2.7 SNMP Config Menu Command

Configuration

Select the check boxes of the entries according to the SNMP functionality you want to use. SNMP version 3 allows permissions to be assigned and protocol level, authentication, and encryption. You specify groups and users in the Groups and Users submenus. You can also make entries there if the SNMPv3 enabled check box is not selected, however the entries are not applied.

Notice

When using SNMP version 3, you should disable SNMP V1 and V2c because the security settings of SNMP V3 can be bypassed by access over SNMP V1 or V2c.

Trap Submenu

Here, you enter the IP addresses of up to 10 trap receivers. The SCALANCE W78x sends a trap to all the addresses you enter if their Enable trap check boxes are selected.

Note

During a warm or cold restart with a wireless connection (AP client, WDS, or WRED), there is no guarantee that the recipient can be reached at the time when the trap is sent. This leads to a loss of the message.

Groups Submenu

This page displays the SNMPv3 groups. You can create a new group by clicking the *New* button and specifying the group name, the security level, and the write or read permissions.

You can delete a group by selecting the check box in the *Del* column and clicking the *Set Values* button. If members are already entered in the group, you cannot delete the group nor is it possible to change the security level of the group.

There are three SNMPv3 security levels:

Security Level	Special Features	Comment
None	No authentication, no encryption.	
Auth/No Priv	Authentication with the MD5 or SHA algorithm, no encryption.	To display the members of the group, you must enter the authentication password (maximum of 63 characters).
Auth/Priv	Authentication with the MD5 or SHA algorithm, encryption with the DES3 algorithm.	To display the members of the group, you must enter the authentication password (maximum of 63 characters).

Users Submenu

This page displays the SNMPv3 users. You can create a new user by clicking the *New* button and specifying the user name and the group to which the user will belong. If necessary, you must also enter the passwords for the authentication and for the encryption.

You can delete a user by selecting the check box in the *Del* column and clicking the *Set Values* button.

Syntax of the Command Line Interface

CLI\SYSTEM\SNMP>

Command	Description	Comment
snmp [E D]	Enables / disables SNMP.	Enables / disables SNMPv1, v2c, v3 and Traps.
snmpv1 [E D]	Enables / disables SNMPv1/v2c.	Enables / disables SNMPv1, v2c and traps.
snmpv3 [E D]	Enables / disables SNMPv3.	The special features of SNMPv3 undertake effect after you disable SNMPv1. Enabling SNMPv3 does not automatically disable SNMPv1.
snmpro [E D]	Enables / disables SNMPv1/v2c read only.	
getcomm [Read community string]	Specifies the Read community string, maximum length 63 characters.	The default is <i>public</i> .
setcomm [Write community string]	Specifies the Write community string, maximum length 63 characters.	The default is <i>private</i> .
traps [E D]	Enables / disables SNMPv1 traps.	Traps are then enabled, if SNMP v1, v2c is also enabled.

CLI\SYSTEM\SNMP\GROUP>

Command	Description	Comment
add <Name> [NOAUTH AUTH PRIV] [R W]	Adds an SNMPv3 group. NOAUTH – No authentication, no encryption; AUTH - Authentication with MD5 or SHA algorithm, no encryption. PRIV - Authentication with MD5 or SHA algorithm and encryption with the DES3 algorithm. R – Read access; W - Write access	Write access without read access is not possible.
edit <Index> [NOAUTH AUTH PRIV] [RE RD WE WD]	Changes the security level of the group and sets the access rights. You can view of the index of the group with the "info" command. RE – allows read access; RD – denies read access; WE – allows write access; WD – denies write access;	You cannot edit the authentication and encryption settings unless the group is empty. Preventing read access also prevents write access. Permitting write access also permits read access.
delete <Index>	Deletes the SNMPv3 group from the group list at the index position.	Is only possible to delete a group if it is empty.
clearall	Clears all SNMP groups that are empty.	

CLI\SYSTEM\SNMP\USER>

Command	Description	Comment
add <user name> <group name> [NONE MD5 SHA] [authentication ID] [Encryption ID]	Assigns an SNMPv3 user to a group. If authentication is necessary for the group, the algorithm must be specified as a parameter (MD5 or SHA). If encryption is necessary for the group, the encryption password must be specified as a parameter.	The authentication password and the encryption password can be a maximum of 63 characters long.
edit <index> <group name> [NONE MD5 SHA] [authentication ID] [Encryption ID]	Changes the group assignment, the authentication algorithm, and the encryption password of the SNMPv3 user.	
delete <Index>	Deletes an SNMPv3 user from the list at the point identified by the index.	
clearall	Deletes all SNMPv3 users.	

CLI\SYSTEM\SNMP\TRAP>

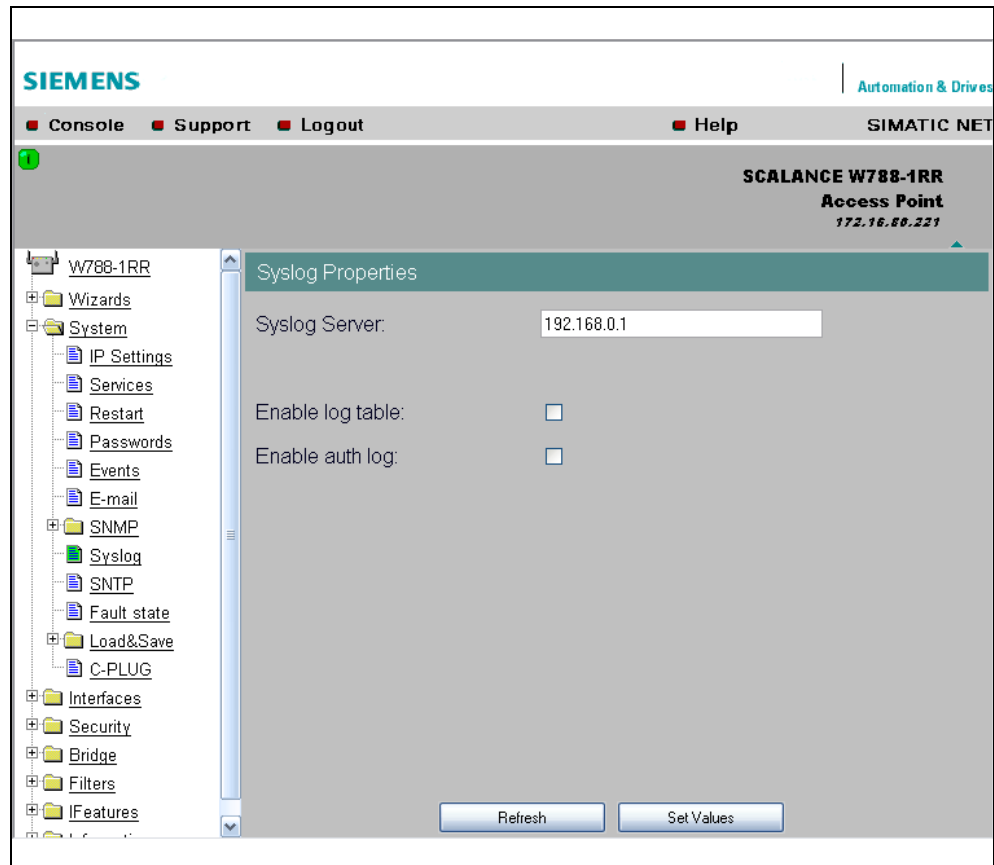
Command	Description	Comment
traps [E D]	Enables / disables SNMP traps.	Traps are then enabled, if SNMP v1, v2c is also enabled.
settrap <entry> <IP address> <E D>	Specifies the IP address of the trap recipient <i>entry</i> (<i>entry</i> between 1 and 10) and enables / disables the sending of traps to this recipient.	

6.2.8 Syslog Menu Command

Syslog according to RFC 3164 is used for transferring short, unencrypted text messages in the IP network. This requires a standard Syslog server.

Syslog Configuration with the SCALANCE W

The parameters used for the Syslog protocol are displayed and set in the System -> Syslog menu:



The meaning of the parameters is as follows:

Syslog Server text box:

The server address decides the IP address to which the Syslog messages are sent. If no IP address is entered in this box, no Syslog messages are sent. If the Syslog server is not in the same network as the SCALANCE W, an automatic attempt is made to establish a connection over the default gateway.

log table check box:

This check box decides whether all entries made in the log table are also sent as Syslog messages.

auth log check box:

This check box decides whether all entries made in the authentication log are also sent as Syslog messages.

Syntax of the Command Line Interface

CLI\SYSTEM\SYSLOG>

Command	Description	Comment
info	Displays the current Syslog configuration.	
server [IP address]	Specifies the IP address of the Syslog server.	Can only be changed with Admin rights.
logs [D E]	Specifies whether the log entries are also sent to the Syslog server.	Can only be changed with Admin rights.
auths [D E]	Specifies whether the authentication log entries are also sent to the Syslog server.	Can only be changed with Admin rights.

6.2.9 SNTP Config Menu Command

Time-of-Day for Synchronization in the Network

SNTP is the acronym for **S**imple **N**etwork **T**ime **P**rotocol. An SNTP server uses this protocol to provide a uniform time throughout the entire network. Clients can synchronize themselves with this time.

If you enter the IP address of an SNTP server here and select the time zone of the SCALANCE W78x, the SCALANCE W78x uses the time information from the server. The SCALANCE W78x adopts this time information without any further conversion regarding daylight-saving or standard time.

Syntax of the Command Line Interface

CLI\SYSTEM\SNTP>

Command	Description	Comment
server [IP address]	Specifies the IP address of the SNTP server.	
tzone [hours]	Specifies the deviation of the time zone of the SCALANCE W78x according to UTC (Universal Time Conversion) in hours.	

6.2.10 Fault State Menu Command

Information on Errors/Faults

This page displays information on faults/errors that have occurred. You can delete this information if you click on the *Remove Fault State* button.

CLI\SYSTEM\FAULT>

Command	Description	Comment
fault [OFF]	Display the fault status and cause of the fault.	You can reset the LED and the fault status with the command: "fault OFF". Ideally, however, the cause of the problem should be eliminated.
ipacknow [Index All]	Displays or acknowledges (clears) the IP Alive messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault state and the Fault LED are cleared if the only reason was an IP Alive error message. The command is not visible in the client mode.
linkack [Index All]	Displays or acknowledges (clears) the Link Check messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault state and the Fault LED are cleared if the only reason was a Link Check error message. The command is not visible in the client mode.

6.2.11 Load & Save Menu Command

Saving and Loading Device Data

Clicking the Load & Save menu command first opens a page with the current firmware version. The *HTTP* and *TFTP* submenus allow you to save device data in external files or to transfer data from external files to the SCALANCE W78x. If the device is operated with a C-PLUG, the data from the loaded configuration file is stored on the C-PLUG. As long as the C-PLUG is inserted, the device works with the configuration on the C-PLUG.

You can save the following device data in external files:

- the configuration data of the SCALANCE W78x
- the content of the log table
- the firmware of the SCALANCE W78x
- the client certificate (only in *client* mode)
- the server certificate (only in *client* mode)

You can transfer the following data from external files to the SCALANCE W78x:

- the configuration data of the SCALANCE W78x
- the firmware of the SCALANCE W78x
- the client certificate (only in *client* mode)
- the server certificate (only in *client* mode)

For information on certificates, please refer to the *System Manual Basics of Industrial Wireless LAN*.

Note

When you download the configuration data to a SCALANCE W78x, a restart is performed so that the new data is adopted correctly. The restart takes place automatically during the loading of HTTP and TFTP. The device can no longer be reached using the old IP address if the downloaded configuration data contains a new IP address.

Note

As of firmware version V3.0, the file with the configuration data of the AP also includes the following information

- Version of the configuration file
- Firmware version with which this configuration file was created
- Order number (MLFB) of the device with which the configuration file was created

It is necessary that the configuration on the C-PLUG was generated with a firmware version \leq the firmware version on the destination device.

Example:

Configuration files generated with a device with firmware version V2.4 or older, can be loaded on devices with firmware version V3.0 without causing problems. Configuration files generated with a device with firmware version V3.0, cannot, however, be loaded on devices with firmware version V2.4 or older.

Reusing Configuration Data

Saving and reading in configuration data reduces the effort if several SCALANCE W78x devices have the same configuration and when IP addresses are obtained over DHCP. Save the configuration data on a PC after you have configured a SCALANCE W78x. Download this file to all other SCALANCE W78x devices you want to configure. If necessary, you may need to assign an IP address to this SCALANCE W78x first using the Primary Setup Tool.

How to Load or Save Data over HTTP / HTTPS

1. Specify the name of the file from which the data will be taken or where the data will be saved in the relevant text box for the configuration data or firmware. As an alternative, you can also use a file selection dialog that opens after you click the *Browse...* button.
2. Start the save function by clicking the *Save* button. Start the load from file function by clicking the *Load* button.

How to Load or Save Data over TFTP

1. Enter the IP address of the TFTP server in the *TFTP Server IP* text box.
2. Enter the port of the TFTP server in the *Port* text box in the default value does not meet your requirements.
3. Click on the Set Values button before you enter any further information for saving the data.

4. Specify the name of the file (maximum 32 characters) from which the data will be taken or where the data will be saved in the relevant text box for the configuration data or firmware.
- 5 Start the save function by clicking the **Save** button. Start the load from file function by clicking the **Load** button.

Configuration Package

If security certificates for the client and/or server are installed on a client, when the configuration is saved, the client provides the option of saving the configuration file with the certificates as a configuration package. With the aid of the configuration package, clients can be replicated simply; in other words, identical settings AND certificates are transferred to the clients in one step. Just as when you download the configuration file, this is followed by a restart. No special measures are necessary when downloading the configuration because the SCALANCE W automatically recognizes the type of configuration file. As a result, it is only possible to assign one common name for the configuration file or configuration package.

Syntax of the Command Line Interface

CLI\SYSTEM\LOADSAVE>

Command	Description	Comment
fwname <i>[file name]</i>	Specifies the name of a file from which the firmware will be loaded or in which the firmware will be saved. This name can be a maximum of 32 characters long.	
fwload	Loads the firmware from a file.	
fwsave	Saves the firmware in a file.	
cfgname <i>[file name]</i>	Specifies the name of a file from which the configuration data will be loaded or in which the configuration data will be saved.	
cfgload	Loads the configuration / configuration package from a file.	
cfgsave	Saves the configuration data in a file.	
logname <i>[file name]</i>	Specifies the name of a file in which the log table will be saved.	
logsave	Saves the log table in a file.	
server <i>[IP address]:[port number]</i>	Specifies the IP address and the port of the TFTP server.	
cltcert <i><certificate></i>	Specifies the name of the certificate for the client.	In client mode only.
cltpass <i><password></i>	Authorizes use of the certificate,	In client mode only.
cltload	Downloads the client certificate from a file.	In client mode only.

Command	Description	Comment
cltsave	Saves the client certificate in a file.	In client mode only.
svrcert <certificate>	Specifies the name of the certificate for the server.	In client mode only.
srvload	Downloads a server certificate from a file.	In client mode only.
srvsave	Saves the server certificate in a file.	In client mode only.
cltdel	Deletes the client certificate.	In client mode only.
srvdel	Deletes the server certificate.	In client mode only.
pkgsave	Saves the Configuration Package in a file over a TFTP server.	In client mode only.

Note

The functionality can be controlled over SNMP with the OID 1.3.6.1.4.1.4196.1.1.4.100.1.5.1.19 (snDownloadEcmCfgPackageControl). Working with this function is analogous to working with the other OIDs in this group.

6.2.12 C-PLUG Menu Command

Information on the Content of the C-PLUG

This menu command provides you with detailed information on the C-PLUG. You can also format the C-PLUG or provide it with new content. As soon as the device is started with a C-PLUG inserted, the SCALANCE W starts up with the configuration data on the C-PLUG. Changes to parameters are stored on the C-PLUG and displayed over the Web and CLI.

The data in the memory of the device only becomes accessible when the device restarts without a C-PLUG using the <Restart without C-PLUG> function.

The screenshot shows the Siemens SCALANCE W788-1RR web interface. The left sidebar contains a tree view with categories like W788-1RR, Wizards, System, IP Settings, Services, Restart, Passwords, Events, E-mail, SNMP, Syslog, SNTP, Fault state, Load&Save, C-PLUG, Interfaces, Security, Bridge, Filters, IFeatures, and Information. The main content area is titled 'C-PLUG Status and Information'. It contains the following fields:

- Device Boot From: C-PLUG (OK)
- C-PLUG State: ACCEPTED
- C-PLUG Device Group: SCALANCE W-700
- C-PLUG Device Type: SCALANCE W788-2PRO
- Configuration Revision: 1
- File System: SIMATIC NET FS
- File System Size (Bytes): 4194304
- Usage (Bytes): 20100
- C-PLUG Info String: 6GK5788-2ST00-2AA6
SCALANCE W788-2PRO
SW: T 2.0.44
HW: 1

At the bottom, there is a 'Modify C-PLUG' dropdown menu with the following options:

- Copy internal Configuration to C-PLUG
- Copy internal Configuration to C-PLUG
- Load default Config to C-PLUG and Restart
- Clean C-PLUG (Configuration on C-PLUG lost)
- Create PRESET-PLUG

A 'Refresh' button is located at the bottom right of the main content area.

C-PLUG State text box

This displays the status of the C-PLUG. The following are possible:

- **ACCEPTED**
A C-PLUG with a valid and suitable content is inserted in the device.

- **NOT ACCEPTED**
C-PLUG missing or invalid or incompatible content of an inserted C-PLUG. The status is also displayed when the C-PLUG was formatted during operation.
- **NOT ACCEPTED, HEADER CRC ERROR**
A C-PLUG with a bad content is inserted.
- **NOT PRESENT**
No C-PLUG is inserted in the device.

C-PLUG Device Group text box

Indicates the SIMATIC net product line that used the C-PLUG in previous operation.

C-PLUG Device Type text box

Indicates the device type within the product line that used the C-PLUG in previous operation.

Configuration Revision text box

The version of the configuration structure. This information relates to the configuration options supported by the device and has nothing to do with the concrete hardware configuration. This revision information does not therefore change if you add or remove modules or extenders, it can, however, change if you update the firmware.

File System text box

Displays the type of file system on the C-PLUG.

File System Size text box

Displays the maximum storage capacity of the file system on the C-PLUG.

File System Usage text box

Displays the memory utilization of the file system of the C-PLUG.

C-PLUG Info String text box

Here, you will see all the additional information about the device that used the C-PLUG during previous operation, for example, order number, type designation, and the versions of the hardware and software.

Modify C-PLUG list box, Modify button

You can only make settings in this box if you are logged on as *administrator*. Here, you decide how you want to change the content of the C-PLUG. The following alternatives are possible:

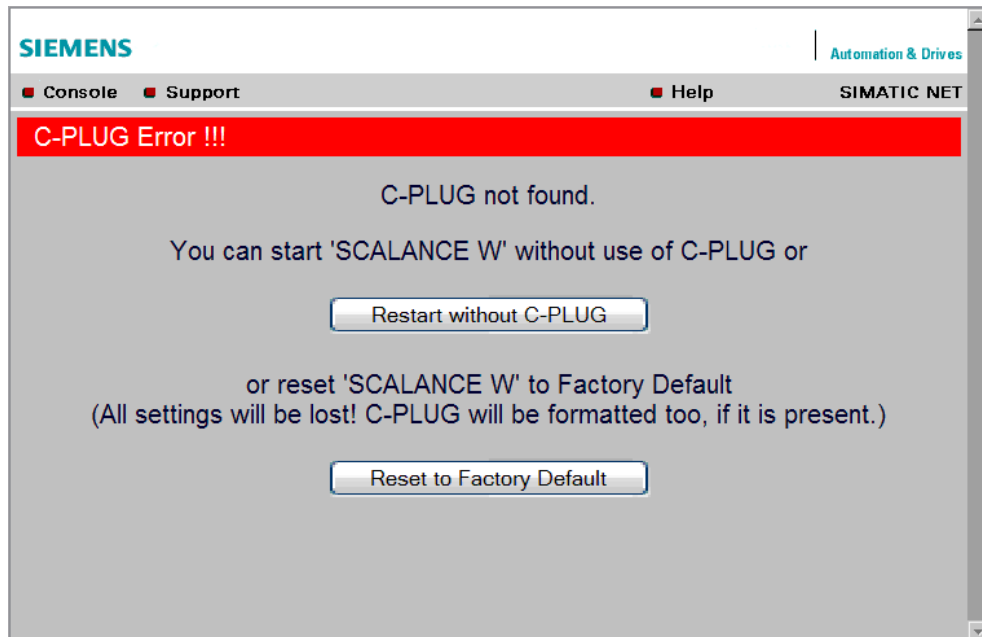
- **Copy internal Configuration to C-PLUG**
The configuration in the internal flash memory of the switch is copied to the C-PLUG; this is followed by a restart.
There is one important use case for this function: The device has started up with a C-PLUG containing a bad configuration or a configuration different from the device. If you have not yet made any configuration changes after starting up the device, you can use this function to overwrite the content of the C-PLUG with the original device configuration.
- **Load default Configuration to C-PLUG and Restart**
A configuration with all the factory default values is stored on the C-PLUG. This is followed by a restart in which the SCALANCE W78x starts up with these default values.
- **Clean C-PLUG (Low Level Format, Configuration lost)**
Deletes all data on the C-PLUG and starts a low-level formatting function. There is no automatic restart.
- **Create PRESET PLUG**
Writes configuration data to a PRESET PLUG. For detailed information on this topic, refer to Section 3.4

After making your selection, start the function by clicking the *Modify* button.

C-PLUG Error Message

If the SCALANCE W78x detects a C-PLUG error during startup, a message is displayed by Web Based Management. C-PLUG errors can have two causes:

- The C-PLUG contains bad data or data for a different device type.
- There is no C-PLUG in the SCALANCE W78x although a C-PLUG was present prior to the last shutdown of the device.



Syntax of the Command Line Interface

CLI\SYSTEM\CPLUG>

Command	Description	Comment
initdef	Reinitializes the C-PLUG and copies the default configuration to it.	All information is deleted.
initmem	Reinitializes the C-PLUG and copies the configuration currently stored internally to it.	All information is deleted.
bootfrom [MEMORY]	Displays the source medium from which the configuration is currently being read: C-PLUG or MEMORY. The restart is performed automatically.	If the C-PLUG was removed, you must specify that the configuration must be read from internal memory. If a C-PLUG is inserted, the system or as attempts to read the configuration from it. The <i>bootfrom [MEMORY]</i> command then has no effect.
preplug <dev>	Writes configuration data to a PRESET PLUG. The <i>index</i> parameter specifies the device for which the PRESET PLUG will be suitable: 1 SCALANCE W788-1PRO 2 SCALANCE W788-2PRO 3 SCALANCE W788-1RR 4 SCALANCE W788-2RR 5 SCALANCE W744-1PRO 6 SCALANCE W746-1 PRO 7 SCALANCE W747-1RR 8 IWLAN/PB Link	

6.3 Interfaces Menu

Introduction

The SCALANCE W78x has one Ethernet interface and up to two WLAN interfaces that can be configured separately. In the pages of this menu, you can configure both the wired Ethernet interface and the WLAN interface.

With the menu command *Interfaces > WLAN1...2 > Virtual AP count* in the *Access Point* mode, you can also configure up to eight virtual access points (VAP0 ... VAP7) per wireless interface.

Note

VAPs are visible only after an AP count > 0.

6.3.1 Ethernet Menu Command

Transmission Speed and Mode

For a wired Ethernet interface, you only to specify the transmission speed / mode parameters and the crossing over of the Ethernet connection. When you select the entry *Auto* in the *Speed / Mode* list box, the SCALANCE W78x sets a suitable speed and mode depending on the other network nodes and crosses over the Ethernet connection.

If you select an entry other than *Auto* in the *Speed / Mode* list box, you must specify the crossing over of the Ethernet connection manually with *Ethernet crossing*.

Note

If you specify the mode, you must make the same settings on the partner device.

Syntax of the Command Line Interface

CLI\INTERFACES\ETHERNET>

Command	Description	Comment
ethspeed [A 100F 100H 10F 10H]	Specifies the transmission speed and mode of the Ethernet interface: A automatic selection by the SCALANCE W788 100F 100 Mbps full duplex 100H 100 Mbps half duplex 10F 10 Mbps full duplex 10H 10 Mbps half duplex	
ethcross [E D]	Manual selection of Ethernet interface crossover. Possible only when ethspeed is not set to auto.	

6.3.2 WLAN Menu Command

Enabling the Interface

Enabling interface by selecting *Enable Interface*.

Network name (only in access point mode)

Enter the network name of the wireless network in the *SSID* text box. If you have used the Basic Wizard, a value is already entered here.

Infrastructure / Ad Hoc (only in client mode)

Select Infrastructure to connect to an access point. Ad hoc is used to connect clients with each other without an access point. This is only possible when ad hoc is set on all clients.

Transmission Mode

Specify the transmission mode in the *Wireless Mode* list box. If you have used the Basic Wizard, a value is already entered here.

Note

IEEE 802.11h transmission (only in Access Point mode):

It is not possible to select the 802.11h protocol in all country settings. It is specified by the configuration of Country code on the System page.

If the 802.11h protocol is selected, after applying the configuration with Set Values, the comment (DFS is active for this country code) appears behind the Enable Interface check box.

With the automatically enabled Dynamic Frequency Selection function (DFS), prior to communication, the access point checks whether configured or selected channel (see Auto Channel Select) is free of signals from a primary user (for example radar).

If signals of a primary user are found on the configured or selected channel, the access point follows the procedure outlined below:

- *Auto channel select* = enabled
With automatic channel select, the access point changes to a different channel and repeats the availability check for this channel.
- *Auto channel select* = disabled
If the channel is fixed in the configuration, the access point changes to the configured alternative channel and repeats the availability check for this channel. If a primary user (for example radar) is discovered on the alternative channel, a further channel is selected at random.

Communication with clients is started only when no primary user has been discovered on the selected channel for one minute.

Outdoor AP mode (*Access Point* mode) / Outdoor Client mode (*Client* mode)

The SCALANCE W78x can be operated either in the indoor or outdoor AP mode. In indoor AP mode, all the country-dependent permitted channels and transmit power settings are available for operation in a building. In outdoor AP mode, the selection of country-dependent channels and the transmit power for operation are restricted for outdoor use. If the SCALANCE W is operated outdoors, make sure that the device is not exposed to rain (installed under a roof) and is not exposed to direct sunlight (installed with UV protection). You enable this mode by selecting *Outdoor AP mode*.

Channel Selection

Select the *Auto Channel Select* check box if you want the SCALANCE W78x to search for a free channel itself. If you want to specify a specific channel, make sure that *Auto Channel Select* is not selected. You can specify a suitable channel in the *Radio Channel* list box.

Auto Channel Select does not exist in the client mode. You can only set a channel in the ad hoc mode.

IEEE 802.11h transmission:

If you have selected the 802.11h protocol for transmission in access point mode and *Auto Channel Select* is not selected, the *Alt. radio channel* input box is displayed below *Radio channel*. Here, you can select the alternative channel in case signals of a primary user are found on the main channel.

Make sure that the alternative channel is not being used by other access points.

In the IEEE 802.11h transmission mode, it is not practical to select the WDS mode at the same time. In WDS mode, all SCALANCE W78x devices must use the same channel. If a signal from a primary user is detected by an AP, the channel is changed automatically and the existing connection is then terminated.

MAC Address of the Client (only in client mode)

A MAC address must be specified for the devices connected to the Ethernet port of the SCALANCE W74x client before it can be reached. This MAC address is used by the client for wireless communication with the access point. This can be done automatically by the client adopting the MAC address of the first frame that it receives over the Ethernet interface. If this is required, *Auto find Adopt MAC* must be selected.

As long as the client is waiting for an Ethernet frame, it registers with the access point using its own MAC address. As soon as the first Ethernet frame is received, the client deregisters from the access point and immediately registers again with the MAC address from the Ethernet frame. If there is now a link-down on the Ethernet port, the client deregisters from the access point and registers again with its own MAC address.

If several devices are connected to the client, you should not select this setting.

You also have the option of specifying the MAC address of the connected device manually. To use this option, select *Set 'Adopt MAC' manually* and enter the MAC address of the device connected to the client in the *Adopt MAC* text box.

To be able to address an entire network of devices downstream from the client, *Adopt own MAC* must be selected. Remember that only layer 3 connections are possible (TCP/IP).

If up to eight MAC addresses need to be served downstream from the client, the layer 2 tunneling setting must be selected for SCALANCE W746-1PRO and SCALANCE W747-1RR.

Note

The layer 2 tunneling functionality is supported by SCALANCE W 788 access points as of firmware version V3.1. This setting meets the requirements of industrial applications in which MAC address-based communication with several devices downstream from the client is required. Clients with this setting cannot connect to standard Wi-Fi devices and SCALANCE W access points with firmware V3.0 or older.

Virtual AP count (only in *access point* mode of a W788xRR)

If you want to configure virtual access points (VAPs) on this AP, set the number of virtual access points using the *Virtual AP count* list box. If *Virtual AP count* = 0 and *VLAN/Prio Tag* is disabled, no VAPs are created.

You can define up to a maximum of 8 VAPs. The settings of VAP0 are made directly in *Interfaces/WLAN*, the settings for VAP1...7 can be found in the *Interfaces/WLAN/VAP1...7* submenus.

By using virtual access points, various SSIDs (maximum of 8 per WLAN interface) can be configured with different security settings. You can assign each virtual AP to a particular VLAN.

Set values

Apply the configuration by clicking *Set Values*.

If you have configured virtual access points (*Virtual AP count* > 0), in *access point* mode, you will be requested to run a restart on the SCALANCE W78x after clicking *Set Values*.

Syntax of the Command Line Interface

CLI\INTERFACES\WLAN1>

or for the second wireless adapter (if it exists)

CLI\INTERFACES\WLAN2>

Command	Description	Comment
port [E D]	Enable / disable wireless port.	
ssid [<i>network name</i>]	Assigns a network name (SSID).	Available only in the access point mode.
mode [A B G H T U X]	Selects the transmission standard: A 802.11a B 802.11b G 802.11g H 802.11h T 802.11a Turbo U 802.11h Turbo X 802.11g Turbo	Depending on the country code, some settings are not possible and will then be rejected. 802.11a Turbo cannot be set in all countries.
autoch [E D]	Enable / disable the channel selection by the SCALANCE W78x.	Available only in the access point mode.
channel [1...167]	Specifies the wireless channel.	
altchan [channel]	Enters the channel number of the alternative DFS channel.	Possible only in 802.11h transmission.
adopt [<i>MAC address</i>]	MAC address of the device connected to the client over Ethernet.	Available only in the client mode.
autoadopt [E D OWN L2T]	Automatic adoption of the MAC address of the device connected to the client over Ethernet. The OWN parameter means that the client registers with the access point with its own Ethernet MAC address. With this setting, however, only IP data traffic is possible.	Available only in the client mode.
adhoc [E D]	Select ad hoc or infrastructure mode.	Available only in the client mode.
anyssid [E D]	With ANY SSID, the client connects to the best access point in the environment in which it is permitted to connect.	Available only in the client mode.
vapno [0...7]	Specifies the number of virtual access points	
outdoor [E D]	Enable / disable outdoor AP mode	
802.11 g	Open the <i>ADVANCED G</i> (802.11g) menu	
ADVANCED	Open the <i>ADVANCED</i> menu	
DATARATES	Open the <i>DATARATES</i> menu	
VAP1	Open the <i>VAP1</i> menu	Displayed only when vapno > 0.

Command	Description	Comment
VAP2	Open the <i>VAP2</i> menu	Displayed only when vapno > 1.
VAP3	Open the <i>VAP3</i> menu	Displayed only when vapno > 2.
VAP4	Open the <i>VAP4</i> menu	Displayed only when vapno > 3.
VAP5	Open the <i>VAP5</i> menu	Displayed only when vapno > 4.
VAP6	Open the <i>VAP6</i> menu	Displayed only when vapno > 5.
VAP7	Open the <i>VAP7</i> menu	Displayed only when vapno > 6.

6.3.3 Advanced Submenu

Configuring Transmission Characteristics

On this page, you can specify details of the transmission characteristics. You only need to adapt the parameters on this page if the SCALANCE W78x cannot be used as it is intended with the default settings.

Transmit Power

In the *Transmit Power* list box, you can specify the output power of the SCALANCE W78x. It may be necessary to reduce the transmit power when using antennas to avoid exceeding the maximum legal transmit power. Reducing the transmit power effectively reduces cell size.

Beacons

Beacons are packets that are sent cyclically by a SCALANCE W78x to inform clients of its existence. In the *Beacon Interval* text box, you specify the interval at which the SCALANCE W78x sends beacons.

Only in the access point mode and with the client in the ad hoc mode

The *Beacon Rate* list box specifies the data rate of beacons. The higher the data rate, the shorter the transmission range.

Only in access point mode

The *Data Beacon Rate DTIM* (Delivery Traffic Indication Map) parameter specifies how often the SCALANCE W78x sends broadcast and multicast packets over the wireless interface. If you enter 1 in this box, the SCALANCE W78x transmits broadcast and multicast packets directly after each beacon (recommended setting for normal network environments). The value 5 would mean that the SCALANCE W78x collects the broadcast and multicast packets and sends them after every fifth beacon.

Increasing this value allows a longer sleep mode for the clients but means a greater delay for broadcast and multicast packets.

RTS/CTS

RTS/CTS (**R**quest **T**o **S**end/**C**lear **T**o **S**end) is a method for avoiding collisions based on the exchange of status information before sending the actual data (Hidden node problem). To minimize network load resulting from the additional protocol exchange, this method is used only when a packet size that you select with the *RTS/CTS Threshold* is exceeded.

Fragmentation

The *Fragmentation Length Threshold* parameter specifies the maximum package size transferred on the radio link. Large packets are divided up into small packets prior to transmission and then reassembled into the original size after they have been received. This can be beneficial if the transmission quality is poor because larger packets are more difficult to transmit. However fragmentation into smaller packets means a poorer throughput.

Repetitions

There are two situations in which packets are repeated. The hardware repetition is performed by the WLAN chip itself when it tries to repeat an unacknowledged packet immediately. The number of attempted repetitions is specified with the *HW Retry number* parameter.

If the number of retries is reached without success, the packet is temporarily withdrawn and all other packets in the buffer are sent first. Following this, transmission of the packet is attempted again. The number of such repetitions is specified with the *SW Retry number* parameter.

Using *Use SW Retry*, the software repetition mechanism can be enabled or disabled.

Shortened Preamble with 802.11b

The 802.11b standard allows the use of shortened preambles in the wireless transmission of data packets. This increases the amount of user data.

Note

If you are using the CP 1515 and CP 7515 communications processors in one wireless cell at the same time, the shortened preamble should not be used otherwise the CP 1515 can only handle a significantly reduced amount of data traffic when there is heavy load on the network.

Antenna Gain

The *Antenna Gain* parameter describes the antenna gain in dBi of an antenna connected to a SCALANCE W.

There are now two boxes that can be selected: "Antenna Gain" and "Antenna Type". If "Antenna Type" is set to "User Defined", any antenna gain can be entered in Antenna Gain. Otherwise, the preconfigured value of the selected "Antenna Type" is displayed.

It is necessary to set a specific value to make sure that the regulations of the national authorities are adhered to. The national authorities, for example, specify all usable channels, the corresponding maximum transmit power and other conditions of use. You will find more detailed information on the regulations in your country using the countrylist.log.

Based on the settings for antenna gain and transmit power, the SCALANCE W automatically selects the permitted channels. Under some circumstances, there may be fewer permitted channels available for antennas with a higher antenna gain than for antennas with a lower antenna gain.

The entries for the Siemens antenna models are supported in the Web interface by an < Antenna type> selection list that automatically enters the correct value in the input box. The values entered automatically take into account the different lengths of the antenna connecting cables shown in the selection list following the type name.

Note

If you select *User defined*, you have the option of entering dBi values as integers for the antenna gain in the range from 0 through 30 dBi. Please remember to take the losses of the antenna connecting cable into account.

Antennas

The *Antenna Mode* list box specifies the use of antennas.

- The *Diversity* setting takes the best of the two antennas for the data transmission. For each WLAN interface, both antennas must be connected. Both antennas should also be of the same type and they should also illuminate approximately the same space. If an access point is operated with the diversity setting and the two antennas span different cells, this can have negative effects.
- With the setting *Tx on A, Rx on B*, antenna A is used to send and antenna B to receive.
- With the setting *Tx on B, Rx on A* antenna B is used to send and antenna A to receive.

With the settings *Diversity*, *Tx on A, Rx on B* and *Tx on B, Rx on A*, both antennas must be connected per WLAN interface. If only one antenna is connected, the connected antenna must be set permanently. The second antenna socket must also have a 50 Ω terminator fitted.

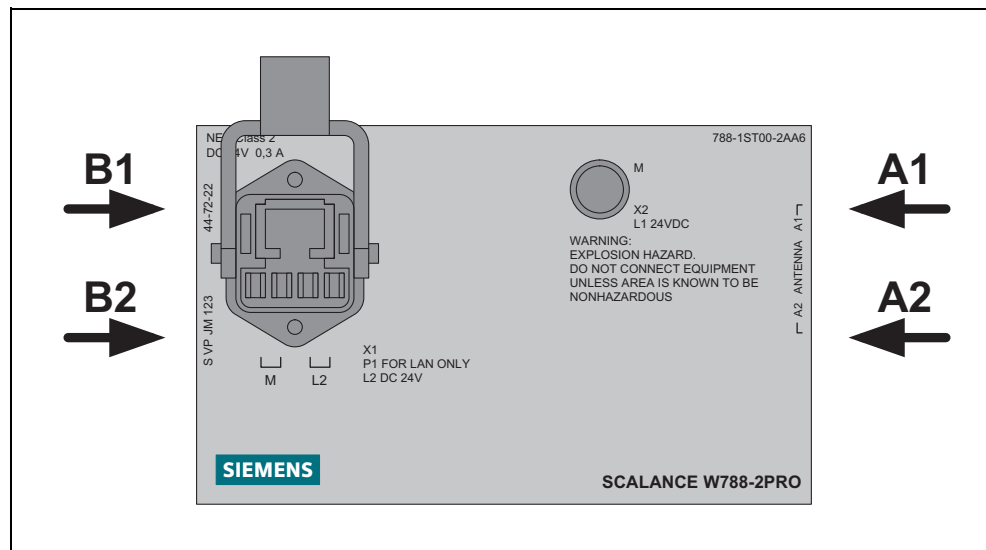


Figure 6-1 Configuration of the Antenna Connectors of the SCALANCE W7xx

Scanning for Access Points (client mode only)

While the client is connected to an access point, it scans for other access points in the background with which it can connect when necessary. There are three modes for scanning access points that can be selected in the *Background scan mode* list box.

If you set *Disable*, there is no scan for access points while the client is connected.

If you set *Scan if Idle*, there is a scan for access points when no data transfer takes place for a certain time.

If you set *Scan Always*, access points are scanned continuously.

The *Background scan interval* parameter specifies the interval at which further access points are scanned.

To optimize the scanning for further access points, you can specify channels for the client on which other access points can be found. To allow this, the *Background Scan Ch.Select* check box must be set and the channels of the other access point are entered in the *Background Scan Channels* text box. Enter the channels separated by blanks.

If the client finds a better access point, it attempts to connect to it. Before it changes, the new access point must be better than the current access point by a certain value. The threshold at which the client changes to the new access point can be specified with the *Roaming threshold* parameter.

Roaming when there is no Ethernet Interface (only in access point mode)

If the wired Ethernet interface is no longer available (cable break, connector removed), a client connected over the wireless network is not aware of this. The SCALANCE W78x can then force the logged on WLAN clients to roam by deactivating its WLAN interface. The client then attempts to log on at a different SCALANCE W78x. You enable this feature by selecting the *Force roaming if link down on Ethernet interface* check box.

Enable WMM (only in access point mode)

With **Wireless Multimedia**, multimedia frames complying with the IEEE 802.11e standard are transmitted at a higher priority (see Section 6.3.2, WLAN > *User priority*).

Select the *Enable WMM* option if you want frames evaluated according to their priority and sent prioritized over the WLAN interface.

According to the Wi-Fi standard, prioritized frames are classified as follows:

Access Category	Description	802.1d Tags
WMM voice priority	Highest priority Allows multiple concurrent VoIP calls, with low latency and toll voice quality	7, 6
WMM Video priority	Prioritize video traffic above other data traffic. One 802.11g or 802.11a channel can support 3-4 SDTV streams or 1 HDTV streams.	5, 4
WMM best effort priority	Traffic from legacy devices, or traffic from applications or devices that lack QoS capabilities. Traffic less sensitive to latency, but affected by long delays, such as Internet surfing.	0, 3
WMM background priority	Low priority traffic (file downloads, print jobs) that does not have strict latency and throughput requirements.	2, 1

Syntax of the Command Line Interface

CLI\INTERFACES\WLAN1\ADVANCED>

Command	Description	Comment
power [0...4]	Specifies by how many dB the transmit power will be reduced compared with full power: 0 Full power 1 -3 dB, half 2 -6 dB, quarter 3 -9 dB, eighth 4 Minimum power, -12 dB	
beacon [20 ... 1000]	Specifies the beacon interval in milliseconds.	
dtim [1 ... 255]	Specifies the data beacon rate.	Available only in the access point mode.
rtsthr [1 ... 2346]	Specifies the packet size as of which RTS/CTS is used.	
fragthr [256 ... 2346]	Specifies the size as of which packets are fragmented.	
bkscan [D I A]	Specifies the mode in which the client scans for further access points. D Disabled I Scan if idle A Scan always	Available only in the client mode.
bkscanint [200...60000]	Interval at which the client scans for further access points.	Available only in the client mode.
bkchannel [channels]	Selection of channels on which the client scans for further access points. The channels are entered separated by blanks.	Available only in the client mode.
bkchsel [E D]	Enables / disables scanning for further access points to specific channels.	Available only in the client mode.
force [E D]	Enables / disables roaming if the connection is lost on Ethernet interface.	Available only in the access point mode.
roamthr	Decides the threshold at which the client changes to another AP. low changes at a slightly higher field strength to the AP with the stronger signal. medium changes at a higher field strength to the AP with the stronger signal. moderately changes at a higher field strength to the AP with the stronger signal. high changes at a significantly higher field strength to the AP with the stronger signal. stronger	

Command	Description	Comment
swretry [E D]	Enables / disables the software retry functionality.	
swretno [0 ... 15]	Specifies the number of software retries.	
hwretno [0 ... 15]	Specifies the number of hardware retries.	
preamb [E D]	Enables / disables the short preamble.	When this function is enabled, higher data rates according to IEEE 802.11b are supported (higher performance).
antenna [A B SA SB D]	Specifies which antennas are used: A Only antenna A B Only antenna B SA Antenna A transmits Antenna B receives SB Antenna B transmits Antenna A receives D The best of both antennas (diversity)	With the IWLAN/PB Link with one antenna socket, the default (Antenna A) must not be changed.
noise [A L M H]	Set the noise filter A Automatic L Low M Medium H High	A strong noise filter allows a more stable connection but also a shorter transmission range.
wmm [E D]	Enables / disables frame transmission taking into account priority.	
antgain [0...30]	Set antenna gain in dBi	
anttype [0...n]	Set antenna type:	To see the list, enter "anttype ?".

6.3.4 SSID List Submenu (client mode only)

Note

The *SSID List* menu is available only when you use the SCALANCE W78x in *Client* mode. You can specify the mode in the *System* menu.

Network Attachment of the Client

With this menu command, you can specify how the SCALANCE W78x connects to a network as client:

- If the *Connect to ANY SSID* check box is selected, the SCALANCE W78x in client mode attempts to connect to the network with the best transmission quality and with suitable security settings. If the *Suppress SSID broadcasting* setting is made for an access point, the SCALANCE W78x cannot log on there with the *ANY SSID*.
- If this check box is not selected, the SCALANCE W78x attempts to connect to the network from the SSID list that has the best transmission quality.

An SSID is absolutely necessary in ad hoc networks and iPCF. The maximum number of SSIDs in the SSID list is restricted to 32.

Syntax of the Command Line Interface

CLI\INTERFACES\WLAN1\SSID>

Command	Description	Comment
add <network name>	Adds a network name (SSID) to the SSID list.	Available only in the client mode.
edit <index> <network name>	Changes the network name (SSID) at the index location in the SSID list.	Available only in the client mode.
delete <Index>	Deletes the network name (SSID) from the SSID list at the index location.	Available only in the client mode.

6.3.5 Advanced G Submenu

Properties of the 802.11g Standard

The IEEE 802.11g is upwards compatible with IEEE 802.11b, both use the 2.4 GHz band. In contrast to 802.11b that specifies data rates up to 11 Mbps, 802.11g provides for data rates up to 54 Mbps. The 802.11g standard also uses the OFDM modulation scheme. This technology divides a data packet into several smaller packets that are transmitted at the same time at different frequencies.

Special Options for 802.11g Settings

The options you can set in the *Advanced G* submenu relate to the way in which management and control data (RTS/CTS frames, beacons) are sent in the 802.11g mode. You can also specify that the SCALANCE W78x only supports 802.11g-compatible devices.

Handling 802.11b Clients

The access point automatically detects whether 802.11b clients exist in the environment. To avoid 802.11g packets colliding with 802.11b packets, the access point can use the RTS/CTS method.

With the *802.11g CTS Mode* list box, you specify the use of RTS/CTS (only in the access point mode).

- 0 do not use RTS/CTS.
- 1 always use RTS/CTS with 802.11g packets.
- 2 only use RTS/CTS when there are 802.11b clients in environment.

You can set the data rate for RTS/CTS frames in the *802.11g CTS Rate* list box.

With the *802.11g CTS Type* list box, you specify whether a CTS or RTS/CTS is sent.

802.11g Expansions

With the *802.11g Short Slot Time* parameter, you specify whether or not the short slot time is used. This short slot time should be supported by all newer clients.

With the *802.11g Only Mode* parameter, you can specify that only 802.11g clients can log on at the access point and also that only 802.11g rates are permitted (only in the access point mode). In this mode, only the OFDM modulation method is used. This prevents 802.11b devices from registering. If *802.11g Only mode* is disabled, both 802.11b devices and 802.11g devices can register with the access point.

Syntax of the Command Line Interface

CLI\INTERFACES\WLAN1\802.11G>

or for the second wireless adapter (if it exists)

CLI\INTERFACES\WLAN2\802.11G >

Command	Description	Comment
ctsmode [0 1 2]	Specifies whether the RTS/CTS method is used for 802.11g packets: 0 Do not use CTS. 1 Always use CTS. 2 CTS depending on whether 802.11b clients exist.	Available only in the access point mode.
ctsrates [0 1 2 3]	Specifies the data rate for 802.11g CTS frames: 0 1 Mbps 1 2 Mbps 2 5.5 Mbps 3 11 Mbps	
ctstype [0 1]	Specifies the method for avoiding 802.11g packet collisions: 0 CTS only 1 RTS/CTS	
sslot [E D]	Enables / disables short slot times between data packets.	
only11g [E D]	When this is enabled, only the OFDM modulation technique is supported.	Available only in the access point mode.
overlap [E D]	If this is enabled, 802.11b are also search for on overlapping channels.	Available only in the access point mode.
Optimize [1...4]	Specifies the optimization level for detection of 802.11b clients: 1 IEEE standard method 2...4 proprietary	Available only in the access point mode.

6.3.6 Data Rates Submenu Command (access point mode only)

Variable Setting of the Transmission Rates

From the table showing all available data rates for the current WLAN mode (802.11b, g, a etc.), you can select any combination of these data rates. The access point will then use only the selected transmission rates for communication with the clients.

The "Basic Rate" parameter specifies that a client must be capable of this data rate to be able to connect to the access point.

The screenshot displays the Siemens SIMATIC NET web interface for a SCALANCE W788-1RR Access Point. The left sidebar shows a navigation tree with categories like Wizards, System, Interfaces, WLAN, Security, Bridge, Filters, IFeatures, and Information. The 'Data Rates' option under the WLAN section is selected. The main content area is titled 'Data Rate Settings for Wireless Interface' and contains a table with the following data:

Data Rate	Enabled	Basic Rate
1 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
2 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
5.5 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
6 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
9 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
11 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
12 Mbits	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
18 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
24 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
36 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
48 Mbits	<input type="checkbox"/>	<input type="checkbox"/>
54 Mbits	<input type="checkbox"/>	<input type="checkbox"/>

At the bottom of the table, there are three buttons: 'Refresh', 'Default Values', and 'Set Values'.

Figure 6-2 "edit" Screenshot:

Syntax of the Command Line Interface

CLI\INTERFACES\WLAN1\Data Rates>

Command	Description	Comment																																							
info	The following overview shows you the available transmission rates and their current configuration.																																								
default	Enables the default setting for the current WLAN mode																																								
edit <Rate> <E D> <E D>	<p>Changes the settings for the specified data rate (in Mbps). The two parameters indicate whether the rate should be used or is defined as "Basic Rate".</p> <p>Overview:</p> <table> <thead> <tr> <th>Rate</th><th>Enabled</th><th>Basic Rate</th></tr> </thead> <tbody> <tr><td>1</td><td>X</td><td>X</td></tr> <tr><td>2</td><td>X</td><td>X</td></tr> <tr><td>5.5</td><td>X</td><td>X</td></tr> <tr><td>6</td><td>X</td><td></td></tr> <tr><td>9</td><td>X</td><td></td></tr> <tr><td>11</td><td>X</td><td>X</td></tr> <tr><td>12</td><td>X</td><td></td></tr> <tr><td>18</td><td>X</td><td></td></tr> <tr><td>24</td><td>X</td><td></td></tr> <tr><td>36</td><td>X</td><td></td></tr> <tr><td>48</td><td>X</td><td></td></tr> <tr><td>54</td><td>X</td><td></td></tr> </tbody> </table>	Rate	Enabled	Basic Rate	1	X	X	2	X	X	5.5	X	X	6	X		9	X		11	X	X	12	X		18	X		24	X		36	X		48	X		54	X		<p>Example:</p> <p>The command "edit 5.5 d d" disables the data rate 5.5 Mbps. The screenshot shows the default setting for the 802.11g mode.</p>
Rate	Enabled	Basic Rate																																							
1	X	X																																							
2	X	X																																							
5.5	X	X																																							
6	X																																								
9	X																																								
11	X	X																																							
12	X																																								
18	X																																								
24	X																																								
36	X																																								
48	X																																								
54	X																																								

6.3.7 VAP Submenu Command

Description

You can only complete the pages of the virtual access points VAP1...VAP7 if you have configured virtual access points at the higher level *Interfaces > WLAN (Virtual AP count > 0)*.

On this page, you can assign a separate SSID to the virtual access points; in other words, the access point operates in multiple SSID mode.

SSID

Enter the SSID of the VLAN here.

Make sure that you also store the SSID of this VLAN in the configuration of the client that you assign to this VLAN.

Note

You can configure separate security settings for each virtual access point (see Section 6.4.1, WBM menu *Security > Basic WLAN > WLAN1/2 > VAP1...7*).

The security settings of the VAPs must meet those of the relevant VLANs.

Syntax of the Command Line Interface

CLI\INTERFACES\WLAN1>VAP1>

or for the second wireless adapter (if it exists)

CLI\INTERFACES\WLAN2>VAP1>

Command	Description	Comment
vap [E D]	Enable /disable virtual access point	
ssid [<i>network name</i>]	Assigns a network name (SSID).	

6.4 The Security Menu

Introduction

In this menu, you configure the security settings with which you want to operate your SCALANCE W78x. Apart from selecting the authentication and encryption scheme, this also includes the decision as to whether or not an external Radius server is used and whether access is restricted based on MAC addresses (ACL).

Syntax of the Command Line Interface

CLI\SECURITY>

Command	Description	Comment
mgmteth [E D]	It is only possible to configure the SCALANCE W78x over the wired Ethernet interface (E) or over all interfaces (D).	

6.4.1 Basic Wireless Menu Command

Authentication

Authentication protects the network from unwanted access.

In the *Authentication Type* box, you can choose between the following types of authentication:

- Open System
There is no authentication. Encryption with a fixed key can be selected as an option. You can choose between WEP or AES based on the key length (see Section 6.4.2).

Note

With the SCALANCE W78x in iPCF mode, only this setting is possible.

- **Shared Key**
In Shared Key authentication, a fixed key is stored on the client and access point. This is then used for authentication and encryption. Once again, you can choose between WEP or AES based on the key length (see Section 6.4.2).

Note

When using an open system with encryption or shared key in conjunction with ACL lists, note the information in Section 6.4.3 ACL menu command..

- **WPA**
Secure WPA/RADIUS authentication uses an external RADIUS server (IEEE 802.1x). With this method, the client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. AES or TKIP can be used as a secure encryption method.
- **WPA-PSK**
WPA authentication works without a RADIUS server (IEEE 802.1x). A fixed key (**Pre-Shared Key**) is stored on every client and access point and is used for authentication and further encryption. AES or TKIP can be used as a secure encryption method.

Note

The key can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long. It should be selected so that is complex for example consisting of random numbers, letters (upper-/lowercase), have few repetitions and special characters). Do not use known names, words or terms that could be guessed. If a device is lost or if the key becomes known, the key should be changed on all devices to maintain security.

- **802.1x (Radius)**
Port-related access check over an external RADIUS server (IEEE 802.1x). With this method, the client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. WEP is used as a weak encryption method.

- **WPA2-PSK**
WPA2-PSK is based on the WPA2 standard, WPA authentication, however, operates without a RADIUS server. Instead of this, a key (pass phrase) is stored on every client and access point and this is used for authentication and further encryption. AES or TKIP is used as the encryption method, AES represents the standard method.
- **WPA2**
WPA2 (Wi-Fi Protected Access 2) is a further development of WPA and implements the functions of the IEEE 802.11i security standard. WPA2 uses the additional encryption protocol CCMP that allows fast roaming in mobile ad hoc networks with its preauthentication. A client can log on in advance and several access points so that the normal authentication can be omitted. A RADIUS server is used to authenticate the client with an access point. The client logs on at a RADIUS server based on a certificate (EAP-TLS) or a combination of user name and password (EAP-PEAP or EAP-TTLS / internal authentication method MSCHAPv2). As an option, the RADIUS server then identifies itself to the client using a certificate. Following successful authentication, the client and RADIUS server generate key material that is used for data encryption. AES or TKIP is used as the encryption method, AES represents the standard method.
- **WPA-Auto-PSK**
Setting with which an access point can process both the *WPA-PSK* as well as *WPA2-PSK* type of authentication. This is necessary when the access point communicates with different clients, some using *WPA-PSK* and others *WPA2-PSK*. The same encryption method must be set on the clients.
- **WPA-Auto**
Setting with which an access point can process both the *WPA* and *WPA2* type of authentication. This is necessary when the access point communicates with different clients, some using *WPA* and others *WPA2*. The same encryption method must be set on the clients.

Encryption

Encryption protects the transferred data from eavesdropping and corruption. You can only disable encryption if you have selected *Open System* for authentication. All other security methods include both authentication and encryption.

Encryption Methods

If you have selected Open System including encryption or *Shared Key* as the authentication, you will need to define a key in the *Keys* menu (see Section 6.4.2).

- **WEP (Wired Equivalent Privacy)**
A weak, symmetrical stream encryption method with only 40- or 104-bit long keys based on the RC4 algorithm (Ron's Code 4).

If you have selected WPA-PSK or WPA (RADIUS) as the authentication, the following alternatives are available in the *Cipher* box:

- **TKIP (Temporal Key Integrity Protocol)**
A symmetrical stream encryption method with the RC4 algorithm (Ron's Code 4). In contrast to the weak WEP encryption, TKIP uses changing keys derived from a main key. TKIP can also recognize corrupted packets.
- **AES (Advanced Encryption Standard)**
Strong symmetrical block encryption method based on the Rijndael algorithm that further improves the functions of TKIP.

RADIUS Authentication Method (only for W788 in client mode)

If a client is authenticated over an external RADIUS server, you can use the "RADIUS authentication type" selection list to specify a method for external authentication. As default, the "Auto" value is selected so that the client provides a RADIUS server with all supported methods. Any other selection restricts the support by the client to this one method. This step may be necessary because some RADIUS servers do not evaluate the response of the client completely or correctly.

The following options are available:

- **EAP TLS** **Extensible Authentication Protocol - Transport Layer Security.**
Uses certificates for authentication
- **EAP TTLS** **Extensible Authentication Protocol - Tunnel Transport Layer Security.** After setting up the TLS tunnel, MS-CHAPv2 is used for internal authentication.
- **PEAP** **Protected Extensible Authentication Protocol.** Alternative draft protocol of IETF for EAP-TTLS

Additional Entries for WPA-PSK and WPA2-PSK

To use the WPA-PSK scheme, you must enter a string in the *Pass Phrase* box that is used by the SCALANCE W78x to initialize dynamic key generation. In the *Group Key Update Interval* box, you specify the time after which a new key is generated.

Suppress SSID broadcasting

With the Suppress SSID broadcasting setting, the SCALANCE W78x is only ever accessible to clients that know its SSID. This method can be used to protect the SCALANCE W78x from unauthorized access.

Note

Since no encryption is used for the SSID transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA (RADIUS) or WPA-PSK if this is not possible) provides higher security.

You must also expect that certain end devices may have problems with access to a hidden SSID.

Inter SSID Communication check box

Selecting this check box allows communication between WLAN clients registered at different SSIDs of an access point.

Example 1:	A SCALANCE W788-2xx was defined with different SSIDs for each of the wireless cards.
Example 2:	A SCALANCE W788-1xx is used with multiple SSIDs.

Note

On a SCALANCE W788-2xx, the Inter SSID communication function must be enabled on both WLAN interfaces or on all VAPs to allow communication between the clients with different SSIDs.

Note

If VLANs are configured for the SSIDs, this setting can prevent communication between the SSIDs according to the VLAN rules.

Intracell Communication list box

- *Intracell blocking*
This setting prevents WLAN client communication within an SSID.
- *Ethernet blocking*
This setting prevents WLAN client communication over the Ethernet interface of the access point.
- *Disabled*
This setting enables both WLAN client communication within an SSID as well as WLAN client communication over the Ethernet interface.

To illustrate the situation, there is an overview of the effects of the Inter SSID Communication and Intracell Communication settings below.

Settings		Possible Communication		
Inter SSID communication	Intracell Communication	within an SSID	with another SSID	to the Ethernet network
Enabled	Disabled	x	x	x
Enabled	Intracell blocking		x	x
Enabled	Ethernet blocking	x	x	
Disabled	Disabled	x		x
Disabled	Intracell blocking			x
Disabled	Ethernet blocking	x		

Syntax of the Command Line Interface

CLI\SECURITY\BASIC\WLAN1>

or for the second wireless adapter (if it exists)

CLI\SECURITY\BASIC\WLAN2>

Command	Description	Comment
authent [0 1 2 3 4 5 6 7 8]	Specifies the authentication type. For the parameter <i>n</i> , enter a number between 0 and 4 for the type authentication: 0 Open System 1 Shared Key 2 WPA (RADIUS) 3 WPA-PSK 4 802.1x (RADIUS) 5 WPA2 6 WPA2-PSK 7 WPA-Auto 8 WPA-Auto-PSK	With the authentication types 7 (WPA-Auto) and 8 (WPA-Auto-PSK), the encryption method of WPA and WPA2 or WPA-PSK & WPA2-PSK must be the same.
encrypt [E D]	Encryption enabled / disabled.	
cipher [OFF AUTO WEP AES TKIP]	Specifies the encryption scheme.	
keysrc [0..2]	Select the key source. Enter 0 as the parameter if the key is managed by the server. Enter 1 in the key will be provided by a RADIUS server. Enter 2 if mixed operation is required.	
defkey [1 2 3 4]	Selects the default WEP key.	
wpphase [WPA password]	Enter the WPA-PSK password.	The password can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long.

Command	Description	Comment
grkint [<i>interval</i>]	Specifies the "Group Key Update Intervals" in WPA-PSK.	Interval in seconds, (0; 36...36000), 0 = OFF
supssid [E D]	<i>Enable / disable Suppress SSID broadcasting functionality.</i>	
Intracell communication intracom [D I E]	Disable / Intracell or Ethernet blocking) Disable = no restriction of data traffic Intracell = blocking of data traffic between the clients in the cell Ethernet = blocking of data traffic to Ethernet	
Inter SSID communication ssidcom [E D]	(Enable / Disable communication to other SSIDs) Enable = data traffic with other SSIDs permitted Disable = data traffic with other SSIDs blocked	
username [<i>name</i>]	Specifies the user name for the RADIUS server.	In client mode only.
password [<i>password</i>]	Specifies the password for the RADIUS server.	In client mode only.
chkserver [E D]	Enables / disables authentication of the server.	In client mode only.
radauth [type]	(Set Authentication Type offered by client to: AUTO, EAP_TLS, EAP_TTLS, PEAP)	

VAP

For each virtual access point VAP1 to VAP7, you configure the following security settings described earlier:

- Authentication
- Enable encryption
- Encryption method
- Select the default WEP key
- Enter the WPA-PSK password
- Specify the *Group Key Update Interval* in WPA-PSK.
- Enable *Suppress SSID broadcasting*

Where they apply, all other security parameters are adopted from the *Security > Basic > WLAN1* or *WLAN2* page.

Syntax of the Command Line Interface

CLI\SECURITY\BASIC\WLAN1>VAP1

or for the second wireless adapter (if it exists)

CLI\SECURITY\BASIC\WLAN2>VAP1

Command	Description	Comment
authent [0 1 2 3 4 5 6 7 8]	Specifies the authentication type. For the parameter <i>n</i> , enter a number between 0 and 4 for the type authentication: 0 Open System 1 Shared Key 2 WPA (RADIUS) 3 WPA-PSK 4 802.1x (RADIUS) 5 WPA2 6 WPA2-PSK 7 WPA-Auto 8 WPA-Auto-PSK	With the authentication types 7 (WPA-Auto) and 8 (WPA-Auto-PSK), the encryption method of WPA and WPA2 or WPA-PSK & WPA2-PSK must be the same.
encrypt [E D]	Encryption enabled / disabled.	
cipher [OFF AUTO WEP AES TKIP]	Specifies the encryption scheme.	
defkey [1 2 3 4]	Selects the default WEP key.	
wpphphrase [<i>WPA password</i>]	Enter the WPA-PSK password.	The password can be 8 to 63 ASCII characters or exactly 64 hexadecimal characters long.
grkint [<i>interval</i>]	Specifies the "Group Key Update Intervals" in WPA-PSK.	Interval in seconds, (0; 36...36000), 0 = OFF
supssid [E D]	Enable / disable <i>Close Wireless System</i> functionality.	

6.4.2 Keys Menu Command

Specifying the WEP/AES Key

To allow you to enable the encryption for the Open System and Shared Key authentication methods, you must first enter at least one key in the key table. You can choose between WEP or AES encryption based on the key length. 5 or 13 ASCII or 10 or 26 hexadecimal characters specify a weak WEP key (40/104 bits). 16 ASCII or 32 hexadecimal characters, on the other hand, define a strong AES key (128 bits).

You can also create keys for WDS Redundancy and ACL Private (these are not supported by all clients for ACL).

Note

When operating the CP 7515, note the following when configuring the keys on the SCALANCE W78x:

The ACL key and the WEP/AES key must be of the same length since the CP 7515 only allows a uniform key length. If the Windows-specific program Zero-Config is used even the keys must be the same.

Syntax of the Command Line Interface

CLI\SECURITY\KEYS\WLAN1>

or for the second wireless adapter (if it exists)

CLI\SECURITY\KEYS\WLAN2>

Command	Description	Comment
add <Len> <Key> [<i>index</i>]	Adds at a key at the end or at the specified <i>Index</i> of the table.	Indexes from 5 onwards are private keys
edit < <i>index</i> > <Len> <Key>	Changes the key at the <i>Index</i> location.	
delete < <i>Index</i> >	Deletes the key at the <i>Index</i> location.	
clearall	Deletes all keys.	

6.4.3 ACL Menu Command

Note

The ACL menu is available only when you use the SCALANCE W78x in the access point mode. You can specify the mode in the *System* menu.

Access Rights for Individual Clients

The access control list (ACL) is an assignment of MAC addresses and access rights.

If ACL is enabled, prior to data transfer, the SCALANCE W78x checks whether the necessary permissions for the communication partner (identified by the MAC address) are entered in the ACL table

Note

Since no encryption is used for MAC address transfer, this function can only provide basic protection against unauthorized access. The use of an authentication method (for example WPA (RADIUS) or WPA-PSK if this is not possible) provides higher security.

Enabling the ACL

In Web Based Management, there is a list box for the use of ACL.

To enable ACL, you must set the global release to either *Enabled* or *Strict*:

Enabled

All clients entered in the ACL are handled according to the ACL entry. Clients not entered in the ACL have access to the access point. This setting can be used to deny access by certain clients.

Strict

All clients entered in the ACL are handled according to the ACL entry. Clients not entered in the ACL have no access to the access point. This setting can be used to allow access by certain clients.

Disabled

The access control this is not used.

Changing an Entry in the ACL

Click the relevant MAC address to change the entry in the ACL. With the *Se/* check box, you decide whether or not an ACL entry is used. The *Del* check box is used to delete an entry from the ACL.

New Entry in the ACL

Click the *New* button to create a new entry in the ACL. A page appears on which you can make the necessary settings. Enter the MAC address of the client in the *MAC Address* text box. You specify the access permissions of the client in the *Permission* list box:

Allow

The client has access to the access point.

Deny

The client does not have access to the access point.

Default Key

The client only has access to the access point when it uses the default key for encryption of the data. To allow this, you must specify a valid default key for the SCALANCE W78x (for example in the *WBM Security* menu) that is also used by the client.

Private Key

With this setting, you can use different keys for different clients. You must first create the private keys with the *Keys* menu command. You can select one of these keys in the *Key number* list box. The client only has access to the access point when it uses this private key. For this function, the client must support private keys.

Note

The private key set in the ACL must also be available in the key list on the client. The client must also use this private key for communication in Security->Basic->WLAN (the key must be set), if an open system with encryption or shared key is used.

The private key is used on this connection for the transferred unicast packets intended for the wireless client.

All multicast and broadcast packets are transferred with the public key set on the access point. The wireless client entered in the ACL list must therefore also enter this public key at the same location in its key list as the access point.

Example

In its cell, an access point uses the setting shared key with a 128-bit public key (default key 1) for encryption of the data traffic.

All wireless clients that register at this access point, require this public key at position 1 in their key list for communication.

If access for certain wireless clients is now restricted by the ACL list of the access point on the basis of a private key, the private key must first be stored in the key list of the access point and the client to be restricted.

The next activity is to enter the MAC addresses of these wireless clients in the ACL list of the access point and to give it the private key. If these wireless clients are intended to continue communication, the private key must be set on the wireless client directly under Security->Basic->WLAN and used for the encryption.

Otherwise the clients could receive broadband or multicast packets, but no longer be addressed directly with unicast packets.

Syntax of the Command Line Interface

CLI\SECURITY\ACL\WLAN1>

or for the second wireless adapter (if it exists)

CLI\SECURITY\ACL\WLAN2>

Command	Description	Comment
aclmode [E D S]	Global release of ACL: E Enable D Disable S Strict	Only in access point mode
add <MAC> [A Y K P][key]	Create a new entry in the ACL: MAC MAC address of the client A Allow Y Deny K Default Key P Private Key Key Key index for private key	Only in access point mode
edit <index> [E D] [A Y K P] [Key]	Change an existing ACL entry: index Number of the ACL entry E Enable D Disable A Allow Y Deny K Default Key P Private Key Key Key index for private key	Only in access point mode
delete <Index>	Delete an existing ACL entry: index Number of the ACL entry	Only in access point mode
clearall	Deletes all ACL entries.	Only in access point mode

6.4.4 RADIUS Server Menu Command

Note

The *RADIUS* menu command is available only when you use the SCALANCE W78x in access point mode. You can specify the mode in the *System* menu.

Authentication over an External Server

The concept of RADIUS is based on an external authentication server. A client can only access the network after the SCALANCE W78x has verified the logon data of the client with the authentication server. Both the client and the authentication server must support the EAP protocol (Extensive Authentication Protocol). The SCALANCE W supports the external authentication mechanisms EAP-TLS, EAP-TTLS and PEAP.

Syntax of the Command Line Interface

CLI\SECURITY\RADIUS>

Command	Description	Comment
server [IP address]	Specifies the IP address of the primary RADIUS server.	
server B [<i>IP address</i>]	Specifies the IP address of the backup RADIUS server.	
port [<i>port</i>]	Specifies the port of the primary RADIUS server.	
port B [<i>port</i>]	Specifies the port of the backup RADIUS server.	
Secret [<i>password</i>]	Specifies the password for the primary RADIUS server.	
secret B [<i>password</i>]	Specifies the password for the backup RADIUS server.	
maxreq [<i>max. number</i>]	Maximum number of queries to the RADIUS server.	
maxreq B [<i>max. number</i>]	Maximum number of queries to the RADIUS server. (backup server)	
authprd [<i>time in s</i>]	Period for repeating authentication.	The default is 3600 s.

6.4.5 Access Menu Command

Access Permissions for IP Addresses

In this menu, you specify the access permissions for IP addresses. You can specify whether management access (SNMP, Telnet, WBM) is possible with the defined addresses:

- Management access is possible only with the defined addresses.

Or:

- Management access is possible with all IP addresses not included in the list.

Note

The defined access rights also apply to the PC used for configuration. If you have not entered the local IP address and have set the ACL mode to *Accessed*, no further access to the SCALANCE W78x is possible.

You should also note that the IP address of the client can change if you use DHCP without reservation.

Syntax of the Command Line Interface

CLI\SECURITY\ACCESS>

Command	Description	Comment
access [E D]	Enable / disable access control list.	
statmgmt [A D]	It is possible to access or not possible to access the IP addresses of the access control list (A ccessed / D enied).	
add <IP>	Adds a new IP address	
edit <Index IP> [E D]	Enables / disables the entry in the table specified by the index or IP address.	
delete <Index IP>	Deletes the entry.	
clearall	Clears the access control list.	

6.5 The Bridge Menu

Introduction

A bridge is a network component that connects two networks. A bridge is not dependent on the protocol; management of the data packages is based on the physical address of the network nodes (MAC address).

The SCALANCE W78x provides bridge functionality because it handles data exchange between wired and wireless Ethernet. The following sections describe the functions that are available and how you configure and use them.

Deleting Aged Bridge Information

The SCALANCE W78x saves the information about which MAC address can be reached over which port in a learning table. Entries in this list are deleted automatically when there is no further data transfer for the corresponding MAC addresses. You can decide the length of time after which addresses are deleted if no data is sent using the *Aging Time* parameter on the start page of the *Bridge* menu.

Syntax of the Command Line Interface

CLI\BRIDGE\>

Command	Description	Comment
aging [E D aging time]	Enables / disables automatic deletion of information on the assignment of MAC addresses and ports. With the Aging time parameter, you can change the time.	Values between 10 s and 1,000,000 s are possible for the <i>Aging time</i> . The default is 300 s (5 min)

6.5.1 WDS Menu Command

Note

The *WDS* menu command is available only when the SCALANCE W78x is used in access point mode and iPCF is not activated. You can specify the mode in the *System* menu.

Communication between SCALANCE W78x Devices

In normal operation, the SCALANCE W78x is used as an interface to a network and communicates with clients. There are, however, situations in which several SCALANCE W78x devices need to communicate with each other, for example to extend wireless coverage or to set up a wireless backbone. This mode is possible with WDS (**W**ireless **D**istributed **S**ystem).

Note

With the firmware update to \geq V3.0, the SCALANCE W78x-xRR devices need to be reconfigured if you use WDS or redundancy and use the MAC address and not the *sysName*.

These functions are then based on the MAC address that changed with the introduction of VAPs with V3.0.

Configuration

In the *MAC / sysName* column, enter the MAC address or the system name of the SCALANCE W78x with which you want to communicate. If you select the *Enc* check box, encryption is used.

Note

In WDS mode, the following restrictions apply:

- All SCALANCE W78x devices that will communicate with each other must use the same channel.
 - You can only use the encryption schemes **WEP** and **AES**.
 - If you want to attach a different access point from the SCALANCE W78x over WDS, you must configure the MAC address. Detection using the *sysName* parameter does not work in this situation.
 - In the IEEE 802.11h transmission mode, it is not practical to select the WDS mode at the same time. In WDS mode, all SCALANCE W78x devices must use the same channel. If a signal from a primary user is detected by an AP, the channel is changed automatically and the existing connection is then terminated.
-

To enable the entry, you must select the *Se/* check box.

Syntax of the Command Line Interface

CLI\BRIDGE\WDS\WLAN1>

or for the second wireless adapter (if it exists)

CLI\BRIDGE\WDS\WLAN2>

Command	Description	Comment
add <MAC Name> [SE SD][Key]	Adds a new WDS connection. Enter either a MAC address or a sysName. With the SE or SD parameters, you can enable or disable encryption. If encryption is enabled, the key must also be specified.	
edit <index> [E D] [SE SD][Key]	Changes the WDS connection specified by <i>Index</i> . With [E D], you can enable / disable the connection.	
delete <Index>	Deletes the connection with the specified index.	
clearall	Deletes all WDS connections.	

6.5.2 VLAN Menu Command

Assignment and Management of the VLAN IDs

The *Current VLAN Configuration* dialog displays a table with an overview of the configured VLAN IDs (VID). The assignment of the configured ports of the access point is also displayed as a member of these VLANs.

The *Name* is used to identify an entry within the current table. *Member List* displays 'U' for untagged member of a VLANs or '-' if a port is not member of a VLAN. The sequence is sorted from left to right in ascending order; in other words, according to the ID of the interface (WLAN 1, WLAN 1 VAP 1, WLAN 2 VAP 2... or WLAN 1 WDS 1, WLAN 1 WDS 2...).

Entries in red, indicate members in the table, entries in black indicate the configured port VLAN IDs.

If an interface is member of a VLAN ID, that is not the same as the port VID, frames arriving from Ethernet with this VLAN ID are accepted. Outgoing frames, however, always have the port VLAN ID.

Click on *VID* or *Name* to open the configuration page for VLAN IDs. With *New*, you create a new VLAN ID, with *Refresh*, you can update the table.

Note

The Ethernet interface does not remove VLAN tags from outgoing frames. If the VLAN is active, the WLAN interfaces always remove all VLAN tags from the outgoing frames.

Member List	Meaning
U	If VID equals port VID; in other words untagged frames from WLAN are given this VID.
U	If the port is a member of the VID; in other words, tagged frames from Ethernet are forwarded on this port.
—	If the port is not a member of the VID; in other words, all the frames coming from Ethernet are blocked / discarded with the corresponding VLAN ID. Frames containing unconfigured VIDs and untagged frames are always blocked if the VLAN is active.

Automation & Drives

Console

Support

Logout

Help

SIMATIC NET

1

W788-1RR

Wizards

System

Interfaces

Security

Bridge

WDS

VLAN

VLAN IDs

Ports

Learning Table

ARP Table

Spanning Tree

Storm Thresholds

Filters

IFeatures

Information

SCALANCE W788-1RR

Access Point






172.16.88.221

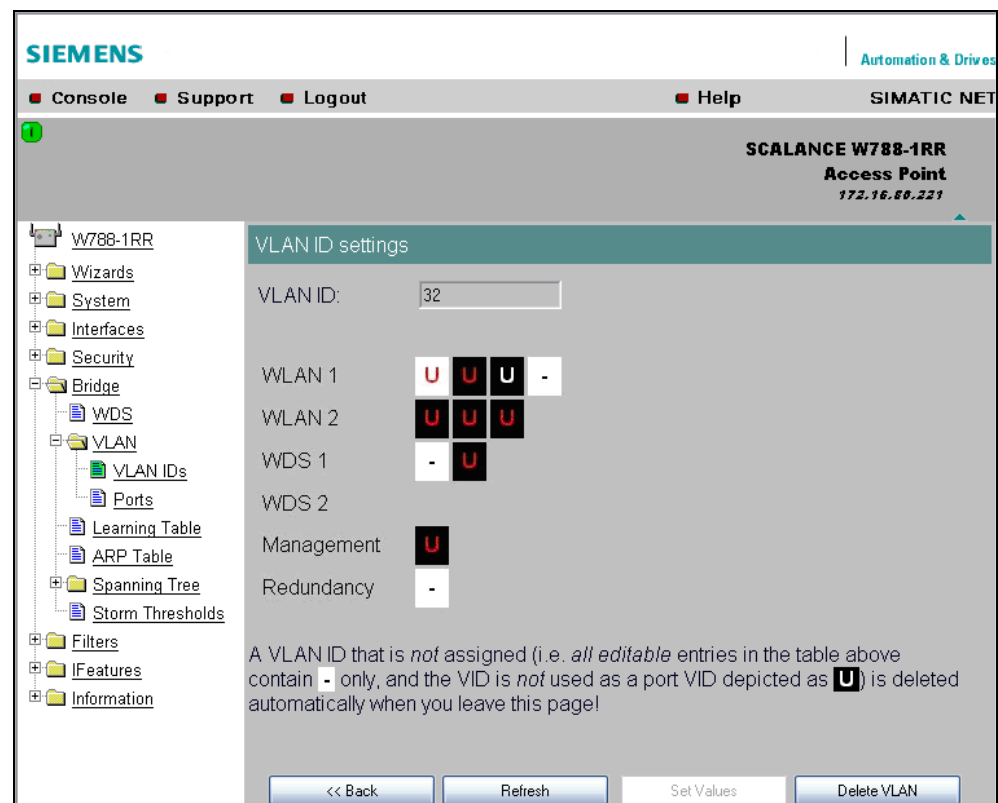
Current VLAN Configuration

VID	Name	Member List					
		WLAN 1	WLAN 2	WDS 1	WDS 2	Mng	Red
30	VLAN 0	UU--	UUU	-U		U	-
31	VLAN 1	-U--	UUU	-U		U	-
32	VLAN 2	UUU-	UUU	-U		U	-
33	VLAN 3	UU-U	UUU	-U		U	-
42	VLAN 4	UU-U	UUU	-U		U	-
50	VLAN 5	-U--	UUU	UU		U	-
120	VLAN 6	-U--	UUU	-U		U	U

VLAN ID Settings

The VLAN ID box allows you to enter a new VID as long as no port is assigned explicitly as member. Otherwise, the VID can no longer be modified.

Representation	Settings	Meaning
1		Field can be edited. If all editable boxes are displayed in this way and if the VID is not configured as port VID, the VID is deleted when you exit this page. Clicking on the field changes to depiction 2.
2		Field can be edited. Clicking on the field changes to depiction 1.
3		Field cannot be edited. All entries for VLAN membership are being used.
4		Field cannot be edited. VID corresponds to the port VID
5		Field cannot be edited. Corresponding port is set to all VLANs,














SIEMENS | Automation & Drives



Console Support Logout Help SIMATIC NET

SCALANCE W788-1RR
Access Point
172.16.66.221

VLAN ID settings

VLAN ID: 32

WLAN 1	   
WLAN 2	  
WDS 1	 
WDS 2	
Management	
Redundancy	

A VLAN ID that is *not* assigned (i.e. *all editable* entries in the table above contain  only, and the VID is *not* used as a port VID depicted as ) is deleted automatically when you leave this page!

<< Back Refresh Set Values Delete VLAN

Ports

Port: Overview of the ports in the form of a table.

SSID: SSID for WLAN interface, no entry for WDS or management and redundancy.

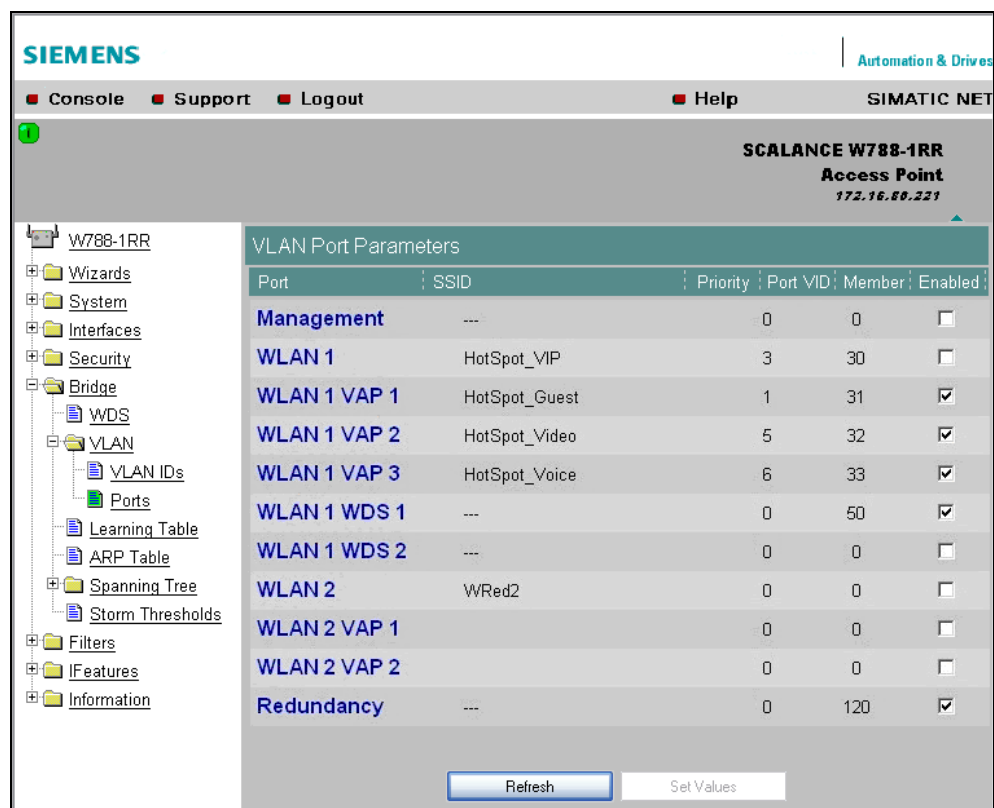
Priority: Configured priority of the port.

Port VID: VLAN ID directly assigned to the port.

Member: The VLAN membership assigned to the port.

Enabled: VLAN support can then be enabled / disabled directly.

Clicking on a port opens the VLAN Settings configuration page.



The screenshot shows the Siemens SCALANCE W788-1RR web interface. The left sidebar contains a tree view with categories like W788-1RR, Wizards, System, Interfaces, Security, Bridge, WDS, VLAN, and others. The main area displays the 'VLAN Port Parameters' table. The table has columns for Port, SSID, Priority, Port VID, Member, and Enabled. The rows include Management, WLAN 1, WLAN 1 VAP 1, WLAN 1 VAP 2, WLAN 1 VAP 3, WLAN 1 WDS 1, WLAN 1 WDS 2, WLAN 2, WLAN 2 VAP 1, WLAN 2 VAP 2, and Redundancy. The 'Enabled' column has checkboxes, some of which are checked.

Port	SSID	Priority	Port VID	Member	Enabled
Management	---	0	0		<input type="checkbox"/>
WLAN 1	HotSpot_VIP	3	30		<input type="checkbox"/>
WLAN 1 VAP 1	HotSpot_Guest	1	31		<input checked="" type="checkbox"/>
WLAN 1 VAP 2	HotSpot_Video	5	32		<input checked="" type="checkbox"/>
WLAN 1 VAP 3	HotSpot_Voice	6	33		<input checked="" type="checkbox"/>
WLAN 1 WDS 1	---	0	50		<input checked="" type="checkbox"/>
WLAN 1 WDS 2	---	0	0		<input type="checkbox"/>
WLAN 2	WRed2	0	0		<input type="checkbox"/>
WLAN 2 VAP 1		0	0		<input type="checkbox"/>
WLAN 2 VAP 2		0	0		<input type="checkbox"/>
Redundancy	---	0	120		<input checked="" type="checkbox"/>

Note

If you use a Radius server for authentication, this must be accessible over the management VLAN. Among other things, the management port also handles the functions: HTTP, HTTPS, WBM, Telnet, SSH, Ping, DHCP, TFTP, SNMP, SNTP and Syslog.

Note

The IP and MAC-based nodes downstream from a client with enabled layer 2 tunneling function (L2T client) adopt the same VLAN properties as the client.

Example: An L2T client is connected to the access point over the WLAN1 VAP3 interface. WLAN1 VAP3 is a member of the VLAN ID 33 that is assigned priority 6. For the L2T port, this means that the devices connected downstream from the L2T client and the client itself are also members VLAN ID 33 with priority 6.

VLAN Settings

VLAN enabled: VLAN support can then be enabled / disabled directly.

User Priority: Prioritization of the data traffic over the port. Untagged frames are given this priority.

Port VLAN ID: Entry of the VLAN ID.

VLAN Membership

All VIDs: Automatic setting of the port as member of all configured VIDs.

Specific VIDs only: Member of up to eight, freely assignable configured VIDs per port.

The screenshot displays the Siemens SCALANCE W788-1RR web management interface. The top navigation bar includes links for Console, Support, Logout, Help, and SIMATIC NET. The main header identifies the device as SCALANCE W788-1RR Access Point with IP 172.16.88.221. A message 'Restart to apply changes.' is visible. The left sidebar shows a tree structure with categories like Wizards, System, Interfaces, Security, Bridge, WDS, VLAN, and others. The 'VLAN' category is expanded, showing sub-items like VLAN IDs, Ports, Learning Table, ARP Table, Spanning Tree, Storm Thresholds, Filters, IFeatures, and Information. The main content area is titled 'VLAN Settings for WLAN 1 VAP 3' and contains the following settings:

- Enable VLAN:** ☒
- SSID:** HotSpot_Voice
- User priority:** 6 - Voice (VO), < 10 ms latency and jitter
- Port VLAN ID:** 33
- VLAN membership:** ☐ all configured VIDs, ☒ specific VIDs only

At the bottom of the settings area are three buttons: << Back, Refresh, and Set Values.

VLAN enable (only in *access point* mode of a W788xRR)

Select the *VLAN enable* option if you want to enable the VLAN function. If *VLAN enable* is selected, all frames of this VAP are given a VLAN tag.

User priority (only in *access point* mode of a W788xRR)

Specify the priority of the frames of this VAP with the *User priority* list box. The priority is evaluated by the connected VLAN-compliant switches (for example, SCALANCE X400) of the network. The priority rises with the ascending numbers:

Note

The priority generally increases with the ascending numbers. The exception is priority 0, that has a higher priority than priority classes 1 and 2 and has the same priority as class 3.

- 0 - *Best Effort (BE)*
normal data traffic
- 1 - *Background (BK)*
non time-critical data traffic
- 2 - *Spare (--)*
this priority is reserved
- 3 - *Excellent Effort (EE)*
data traffic with highest priority
- 4 - *Controlled Load (CL)*
- 5 - *Voice (VI), < 100 ms latency and jitter*
video/multimedia
- 6 - *Voice (VO), < 10 ms latency and jitter*
voice over IP
PNIO
- 7 - *Network Control (NC)*
internal network control frames

Default is 0 - *Best Effort (BE)*.

Note

Both voice over IP and PNIO have priority 6.

Port VLAN ID (only in *access point* mode of a W788xRR)

Here, you enter the VLAN ID (VID) of the VLAN on which the virtual access point will communicate.

The individual VLANs are configured in the VLAN-compliant switches (for example SCALANCE X400). The VID of a VLAN is in the range from 1 to 4094.

VLAN membership (only in *access point* mode of a W788xRR)

Here, you specify the VLANs for which the virtual access point will be a member or which other VLANs the port VLAN ID (VID) entered above will be assigned to.

The following alternatives in the assignment are possible:

- *all*
The VAP is member of all VLANs.
- *only*
The VAP is member only of the VLANs entered below.
Here, enter the VLAN ID (*VID*) of up to 8 VLANs in which the VAP will be a member.

Syntax of the Command Line Interface

CLI\BRIDGEVLAN\VLAN_ID>

Command	Description
info	Shows the currently configured VLANs and their relationship to the ports.
add <VLAN-ID> [u [Ports]]	<p>Inserts a new VLAN.</p> <p>Ports: Specifies the ports configured for the VLAN.</p> <p>u: The port is a member of the VLAN. Frames are sent without VLAN tag.</p> <p>Examples: add 100 u 2 4 Creates an entry with the VLAN ID 100. Ports 2 and 4 are members of this VLAN.</p>
edit <VLAN-ID> [- [Ports],] [u [Ports],]	<p>Changes the membership of ports in a VLAN. The parameters correspond to those of the add command.</p> <p>Examples: edit 100 - 2 Port 2 no longer belongs to the VLAN with ID 100.</p>
delete <VLAN-ID>	Deletes the VLAN with the specified VLAN ID from the configuration of the SCALANCE W78x.

CLI\BRIDGE\VLAN\PORTS>

Command	Description
info	Displays an overview of the ports and corresponding VLAN settings.
vlan <Port> <E/D>	Enables / disables VLAN for the specified port.
portvid <Port> <VLAN-ID>	Received frames without a VLAN tag at the specified port are given a VLAN tag with the <VLAN-ID>.
portprio <Port> <Priority>	The priority assigned to untagged frames according to 802.1d.
member <Port> <all specific>	The specified port is a member of all VLANs or only the VLAN configured in VLAN ID (specific, see above).

6.5.3 Learning Table Menu Command

Assignment of MAC Address and Port

The learning table contains the information about whether a MAC address can be reached over the wired Ethernet interface or over the wireless interfaces. The SCALANCE W78x obtains this information from the active data exchange. The learning table also contains information on clients and on up to 8 devices connected downstream from it operating in the layer 2 tunneling mode.

6.5.4 ARP Table Menu Command

Assignment of MAC Address and IP Address

The ARP protocol (**A**ddress **R**esolution **P**rotocol) obtains the corresponding MAC address of a known IP address. The page of this menu command also indicates the interface over which an address can be reached. The last column indicates how the information was obtained (for example *dynamic* if it was obtained during operation or *static* if it was configured).

6.5.5 Spanning Tree Menu Command

Note

The *Spanning Tree* menu command is available only when you use the SCALANCE W78x in the access point mode. You can specify the mode in the *System* menu.

Avoiding Loops on Redundant Connections

The spanning tree algorithm allows network structures to be created in which there are several connections between two stations. Spanning tree prevents loops being formed in the network by allowing only one path and deactivating the other (redundant) ports for data traffic. If there is an interruption, the data can be sent over an alternative path. The functionality of the spanning tree algorithm is based on the exchange of configuration and topology change frames.

Definition of the Network Topology Using the Configuration Frames

Network components exchange configuration frames known as BPDUs (Bridge Protocol Data Unit) with each other to calculate the topology. The root bridge is selected and the network topology created using these frames. The root bridge is the bridge that controls the spanning tree algorithm for all involved components. BPDUs also bring about the status change of the bridge ports.

Rapid Spanning Tree

The rapid spanning tree algorithm is based on the spanning tree algorithm. This was optimized in terms of the reconfiguration time. Typical reconfiguration times for spanning tree are between 20 and 30 seconds. With rapid spanning tree, the reconfiguration times are around 1 second. This was achieved by the following measures:

- **Edge ports**
A port defined as an edge port is activated after the hello time (the time between two configuration frames). When the hello time has elapsed, the station can be certain that no further configuration frame will arrive and that this port is an edge port. If the user wants to avoid the hello time, spanning tree can be disabled at this port.
- **Point to Point (direct communication between two neighboring stations)**
By directly linking network components, a status change (reconfiguration of the ports) can be made without any delays. A point-to-point connection can, for example, be a WDS connection between two access points.
- **Alternate Port (substitute for the root port)**
A substitute for the root port is configured. If the connection to the root bridge is lost, the station can establish a connection over the alternate port without any delay by reconfiguring.
- **Filter table**
In rapid spanning tree, ports affected by a reconfiguration are immediately deleted from the filter table. With spanning tree, on the other hand, the point at which a port is deleted is decided by the time when the port was entered in the filter table.
- **Reaction to events**
Rapid spanning tree reacts to events, for example an aborted connection, without delay. There is no waiting for timers as in spanning tree.

In principle, therefore with rapid spanning tree, alternatives for many parameters are preconfigured and certain properties of the network structure taken into account to reduce the reconfiguration time.

(Rapid) Spanning Tree Configuration

The parameters used for the (Rapid) Spanning Tree protocol are displayed in the *(Rapid) Spanning Tree Properties* menu.

The screenshot displays the Siemens SIMATIC NET web interface for a SCALANCE W788-1RR Access Point. The left sidebar shows a tree structure with 'Spanning Tree' selected. The main area contains the following configuration parameters:

Parameter	Value
Enable (R)STP:	<input checked="" type="checkbox"/>
Version:	RSTP
Bridge Priority:	32768
Max Age:	20
Hello Time:	2
Forward Delay:	11

Buttons for 'Refresh' and 'Set Values' are located at the bottom of the configuration area.

If necessary, modify the following parameters to specify how the (rapid) spanning tree algorithm operates:

Enable (R)STP Check Box

Select the Enable Spanning Tree check box if you want to use the (rapid) spanning tree algorithm. If the check mark is not set, all ports are automatically in the 'Forwarding' status.

Version list box

The version decides whether the Rapid Spanning Tree protocol (RSTP) is used or whether the device is operated in compatibility mode of the Spanning Tree protocol (STP).

Bridge Priority text box

The identification of the most efficient connection is always related to the root bridge, a network component that can be considered as a root element of a tree-like network structure. With the *Bridge Priority* parameter, you can influence the selection of the root bridge.

The bridge with the highest priority (in other words, with the lowest value for this parameter) becomes the root bridge. If several network components in a network have the same priority, the station whose MAC address has the lowest numeric value will become the root bridge. Both parameters, bridge priority and MAC address together form the *Bridge Identifier*. Since the root bridge manages all path changes, it should be located as centrally as possible due to the propagation time of the frames. The value for the bridge priority is a whole multiple of 4096 with a range of values from 0 through 61440.

Max Age text box

Max Age is the time that a bridge waits for a configuration frame (BPDU). When this time has elapsed, the bridge attempts to reconfigure the network. The default for this parameter is 20 seconds.

Hello Time text box

Each bridge regularly sends configuration frames (BPDUs). The interval between two such frames is the *Hello Time*. The default for this parameter is 2 seconds.

Forward Delay text box

New configuration data is not used immediately by a bridge but only after the period specified in the *Forward Delay* parameter. This ensures that operation is only started with the new topology after all the bridges have the required information. The default for this parameter is 11 seconds.

Syntax of the Command Line Interface

CLI\BRIDGE\SPANNING>

Command	Description	Comment
info	Displays the current Spanning Tree configuration.	
spanning [E D]	Enables (E) or disables (D) the (R)STP algorithm.	
version [R S]	Specifies whether the Rapid Spanning Tree (R) or Spanning Tree (S) mode is used.	
bridge [0 ... 61440]	This specifies the bridge priority for the SCALANCE W:	Default value: 32768
hellotm [1 ... 10]	Specifies the interval between two BPDUs in seconds.	Default value: 2 s
fwd_delay [4 ... 30]	Specifies the delay time for the effectiveness of configuration information (specified in seconds).	Default value: 11 s
maxage [6 ... 40]	Maximum age for configuration information. (specified in seconds)	Default value: 20 s

Spanning Tree Port Settings

Port-Specific Parameters

This page displays the current port parameters. The settings are made either using the automatic function of the SCALANCE W or by the user.

The screenshot shows the Siemens SCALANCE W788-1RR web interface. The left sidebar contains a tree view with categories like W788-1RR, Wizards, System, Interfaces, Security, Bridge, WDS, VLAN, Learning Table, ARP Table, Spanning Tree, Properties, Ports, Storm Thresholds, Filters, IFeatures, and Information. The main content area displays the '(R)STP Port Parameters' table. The table has eight columns: Port, Priority, STP Cost, RSTP Cost, Edge, P.t.P., and Enabled. The 'Enabled' column contains green checkmarks. The table lists parameters for Ethernet, WLAN 1, and WLAN 1 VAP 1 through WLAN 1 WDS 7. At the bottom of the table are 'Refresh' and 'Set Values' buttons.

Port	Priority	STP Cost	RSTP Cost	Edge	P.t.P.	Enabled
Ethernet	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 1	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 2	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 3	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 4	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 5	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 6	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 VAP 7	128	100	0	X	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 1	128	100	0	-	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 2	128	100	0	-	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 3	128	100	0	-	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 4	128	100	0	-	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 5	128	100	0	-	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 6	128	100	0	-	Auto	<input checked="" type="checkbox"/>
WLAN 1 WDS 7	128	100	0	-	Auto	<input checked="" type="checkbox"/>

The eight columns of the port table show the following information:

Port

Specifies the ports to which the information relates. Wireless 1_2, for example, relates to the virtual access point VAP2 on the first WLAN interface.

Priority

With this parameter, you specify the priority of the ports of a bridge.

If the path calculated by spanning tree is possible over several ports of a station, the port with the highest priority (in other words the lowest value for this parameter) is selected. A value from 0 through 255 can be specified for the priority; the default is 128.

STP Cost & RSTP Cost

These parameters are used to calculate the path that will be selected. The lower the value, the greater the probability that the corresponding path will be used. If several ports of a bridge have the same value, the port with the lowest port number will be selected. Depending on whether STP or RSTP was selected as the version, the value of STP Cost or RSTP Cost will be used.

The calculation of the path cost is based mainly on the transmission rate. The higher the achievable transmission rate, the lower the value for Path Cost should be.

Typical path costs for Spanning Tree and Rapid Spanning Tree:

Data Rate	Path costs STP	Path costs RSTP
100 Mbps	19	200.000
54 Mbps	33	370.370
48 Mbps	36	416.667
36 Mbps	43	555.556
24 Mbps	53	833.333
18 Mbps	58	1.111.111
12 Mbps	83	1.666.667
11 Mbps	90	1.818.182
10 Mbps	100	2.000.000
9 Mbps	111	2.222.222
6 Mbps	166	3.333.333
5.5 Mbps	181	3.636.364
2 Mbps	500	10.000.000
1 Mbps	1000	20.000.000

The values can, however, also be sent individually.

Edge

The following entries are possible in this column:

yes

An edge port is connected to this port.

no

A spanning tree or rapid spanning tree device is connected to this port.

If an edge port is connected, a SCALANCE W can switch over the port more quickly without taking into account spanning tree frames. If a spanning tree frame is received despite this setting, the port automatically changes to the *no* setting for further stations.

Note

If clients with the layer 2 tunneling function enabled connect to the access point, a separate port is opened for each of these clients. These ports cannot, however, be configured for Rapid Spanning Tree. The settings (for example, priority and path costs etc.) of the cell over which the client is connected to the access point are adopted.

Example: An L2T client is connected to the access point over the WLAN1 VAP3 (Wireless 1_3) interface. The settings for WLAN1 VAP3 are: priority 128, path costs for STP of 100, path costs for RSTP of 0 and the setting EdgePort enabled (in other words, there is an end device on this port). These settings are adopted for the L2T port with one exception.

The Edge-Port enabled setting is not adopted because layer 2 tunneling clients and the ports downstream from the client can never be edge ports.

P.t.P.

There is a point-to-point link when two RSTP-compliant network components are connected together over this port. There are three possible statuses :

ForceTrue

Even with half duplex, a direct link is assumed.

ForceFalse

Despite a full duplex connection, a point-to-point link is not assumed.

Auto

Point-to-point is detected automatically. If the port is set to half duplex (shared media connection), a direct link is not assumed.

Example: A WDS connection between access points is always a half duplex connection. With the setting ForceTrue, a direct connection is assumed. With Auto, a direct connection is not assumed.

Enabled

Shows whether spanning tree is *enabled* or *disabled* for the port.

Configuration of a Port for (Rapid) Spanning Tree

If you click on a port name in the first column, you open the *(Rapid) Spanning Tree Port Properties* page:

The screenshot shows the Siemens SIMATIC NET web interface for a SCALANCE W788-1RR Access Point. The left sidebar displays a tree view with the following structure:

- W788-1RR
 - Wizards
 - System
 - Interfaces
 - Security
 - Bridge
 - WDS
 - VLAN
 - Learning Table
 - ARP Table
 - Spanning Tree
 - Properties
 - Ports
 - Storm Thresholds
 - Filters
 - IFeatures
 - Information

The main content area is titled "(Rapid) Spanning Tree Port Properties" and contains the following configuration fields:

- Enable (R)STP: ☒
- Priority:
- STP Admin Path Cost:
- RSTP Admin Path Cost:
- Admin Edge Port: ☒
- Admin Point-To-Point:

At the bottom of the page, there are three buttons: "<< Back", "Refresh", and "Set Values".

STP enabled check box

Enable this check box, if you want the port to use the (rapid) spanning tree protocol.

Priority text box

Here, enter a value between 0 and 255 for the port priority.

Admin Path Cost text box

Here, you can enter a value for the STP or RSTP *Path Cost* parameter. The relevant value is then used depending on the selected version.

If you enter a zero for the RSTP value, the value for the path costs is calculated automatically.

Admin Edge Port check box

Enable this check box if an end device is connected to this port, otherwise a reconfiguration of the network will be triggered by every link change.

Admin Point to Point Status check boxes

Here, there are three possible settings:

Shared media Connection is selected:

This corresponds to the entry *ForceFalse* in the port table.

Point to Point Connection is selected:

This corresponds to the entry *ForceTrue* in the port table.

Point to Point Connection and Shared Media Connection are not selected:

This corresponds to the entry *Auto* in the port table.

Note

Point-to-point means a direct connection between two stations. A shared media connection would, for example, be a connection from the Ethernet port to a hub or a WDS connection between two access points.

Syntax of the Command Line Interface

CLI\BRIDGE\SPANNING\PORTS>

Command	Description	Comment
info	Displays the current Spanning Tree configuration for all ports.	
portstp <E D> [ports]	Enables / disables the spanning tree algorithm for the specified ports.	
portprio <Port> [0 ... 255]	Specifies the priority of the port.	Default value: 128
stp_cost <Port> [1 ... 65535]	Specifies the path costs for the port if Version is set to STP.	Default value: 100

Command	Description	Comment
rstp_cost <Port> [0 ... 200000000]	Specifies the path costs for the port if Version is set to RSTP. If the value is 0, the value is calculated.	Default value: 0
edgeport <Port> [T F]	Specifies whether or not an edge port (T) or a station (F) that supports spanning tree or rapid spanning tree is attached to this port. if a (rapid) spanning tree protocol is received, the value F is displayed automatically.	
ptpport <port> <A T F>	<p>The point-to-point link establishes a direct link between two stations. In this case, you have the following options:</p> <p>A The port recognizes a PtP port based on the duplexity. In full duplex, a PtP link is assumed, in half duplex no PtP link is assumed (shared medium).</p> <p>T Specifies a PtP link, even though half duplex is being used.</p> <p>F Specifies that there is no PtP link over the relevant port even with full duplex.</p>	

6.5.6 Storm Threshold Menu Command

Note

Storm Threshold is available in access point and in the client mode. The function can only be used in client mode if NAT is disabled.

Limitation of Broadcast and Multicast Frames

Storm Threshold is the maximum number of broadcast or multicast frames per second forwarded by the SCALANCE W78x. If this limit is exceeded, the SCALANCE W78x stops processing such frames for 30 seconds.

Syntax of the Command Line Interface

CLI\BRIDGE\STORMTHR>

Command	Description	Comment
stormthr <E D>	Enables / disables the storm threshold function.	
broadcast <limit value>	Specifies the maximum number of broadcast packets per second from the same address.	
multicast <limit value>	Specifies the maximum number of multicast packets per second from the same address.	
broad_eth <limit value>	Specifies the maximum number of broadcast packets per second for the Ethernet interface.	
multi_eth <limit value>	Specifies the maximum number of multicast packets per second for the Ethernet interface.	
broad_1 <limit value> broad_2 <limit value>	Specifies the maximum number of broadcast packets per second for the first or second wireless interface.	
multi_1 <limit value> multi_2 <limit value>	Specifies the maximum number of multicast packets per second for the first or second wireless interface.	

6.5.7 NAT Menu Command

Note

This menu command is available only with the following variants:

- SCALANCE W746-1PRO
 - SCALANCE W747-1RR
 - SCALANCE W78x (client mode only)
-

What is NAT?

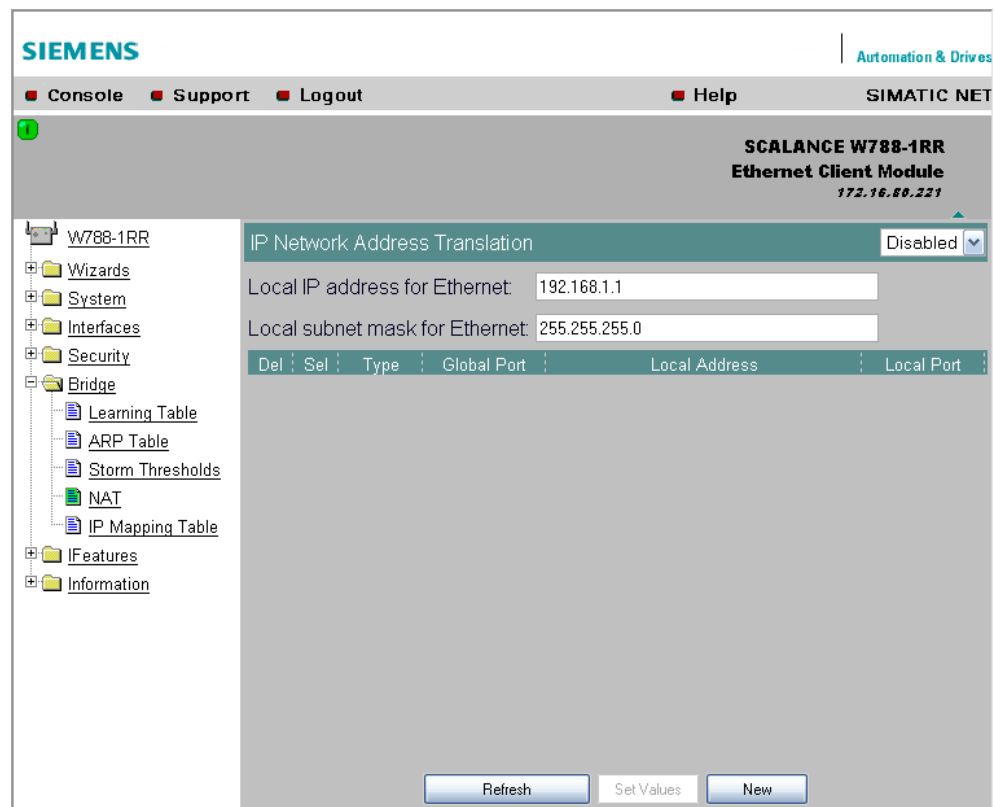
With **Network Address Translation (NAT)**, the IP address in a data packet is replaced by another. NAT is normally used on a gateway between a private LAN and an external network with globally valid IP addresses. A local IP address of the internal LAN is changed to an external global IP address by a NAT device at the gateway.

To translate the internal into the global IP address, the NAT device maintains a translation list.

What is NAPT?

In *Network Address Port Translation (NAPT)* or *Port Address Translation (PAT)*, several internal source IP addresses are translated into the same external source IP address. To identify the individual source nodes, the port of the source device is also stored in the translation list of the NAT gateway and translated for the external address.

If several local clients send a query to the same external destination IP address over the NAT gateway, the gateway enters its own external source IP address in the header of these forwarded frames. Since the forwarded frames have the same global source IP address, the NAT gateway assigns the frames to the clients using different port number.



Note

NAT/NAPT is possible only on layer 3 of the ISO/OSI reference model. To use the NAT function, the networks must use the IP protocol.

When using the ISO protocol that operates at layer 2, it is not possible to use NAT.

NAT Properties of the SCALANCE Devices

When using the WLAN clients SCALANCE W746-1PRO, W747-1RR and W78x (in client mode) as NAT gateways, the WLAN clients must be connected over the Ethernet port with the local Ethernet devices.

The local IP address of the WLAN client on the Ethernet devices must be entered as the gateway address.

The address assignment differs depending on the communication direction:

- From Ethernet device to access point: *Dynamic* address assignment (NAT)
The continuous address assignment is made automatically.
- From access point to Ethernet device: *Static* address assignment (NAPT)
The address assignment is fixed and must be set as a parameter.

32 entries can be set as NAT gateways per WLAN client.

Configuration

Set the configuration on the *IP Network Address Translation* page with the following settings:

- **Enable NAT**
Click the check box *Enable* if you want to enable NAT.
Caution: The change is adopted only after a restart!
- **Local IP**
Here, you enter the local IP address for the Ethernet port of the WLAN client.
- **Subnet Mask**
Enter a subnet mask for the local Ethernet network here, if applicable.
- **Del**
Select the *Delete* check box if you want to delete the previous entries on this page.
- **Sel**
Select the *Select* check box if you want to enable the current entries.
- **Type**
Here, you select the assignment TCP or UDP for the following global port. TCP and UDP frames must have their parameters set separately.
- **Global Port**
Enter the number of the global port (for TCP or UDP).

Note

If the port is already occupied by a local service (for example Telnet), a warning is displayed. In this case, avoid using port 23 (Telnet) and port 80 (http: availability of the client with the WBM) as global port.

- **Local Address**

Here, you enter the local address of the Ethernet device.

- **Local Port**

Here, you enter the number of the local port of the Ethernet device.

Note

The following instructions apply only to the IP parameter assignment using the PST tool.

When the module is accessed with PST by a configuration computer, the address assignment differs depending on the interface:

- PST over the wireless interface:
The *global* address is changed.
 - PST over the Ethernet interface:
The *local* address is changed.
-

Syntax of the Command Line Interface

CLI\BRIDGE>nat

Command	Description	Comment
nat [E D]	Enables/disables NAT	
ip [IP address]	Sets the local IP address for the Ethernet port	
subnet [Subnet mask]	Sets the subnet mask for the Ethernet port	
static	Opens the "STATIC" menu	

CLI\BRIDGE\NAT>subnet

Command	Description	Comment
Local Subnet mask : 255.255.255.0	value of the local subnet mask	

CLI\BRIDGE\NAT>STATIC

Command	Description	Comment
add <type> <G port> <L IP> <L port>	Add the static NAT entry: type = TCP or UDP G port = global port L IP = local IP L port = local port	
edit <Index> <E D> [type] [G port] [L IP] [L port]	Edit the static NAT entry: index = index in table type = TCP or UDP G port = global port L IP = local IP L port = local port	
delete <Index>	Deletes a static NAT entry	
clearall	Deletes all static NAT entries	

CLI\BRIDGE\NAT\STATIC>info

Index	Enabled	Type	Global Port	Local IP	Local Port
1	x	TCP	21	172.27.138.2	1026

Example of static information

6.5.8 IP Mapping Table Menu Command

Note

This menu command is available only with the following variants:

- SCALANCE W78x in client mode
 - SCALANCE W746-1PRO
 - SCALANCE W747-1RR
-

WLAN Access by Several Devices over a Client

With the devices listed in the first paragraph, you can provide access to the WLAN for several devices with one client. This means that you do not need to equip every device with its own wireless client.

This so-called IP mapping is possible only if the connected devices are addressed only by IP frames. Communication at MAC address level (ISO/OSI layer 2) can

- be established with one component whose MAC address is configured on the client,
- be established with a maximum of eight components if the layer 2 tunneling function is selected.

The layer 2 tunneling setting meets the requirements of industrial applications in which MAC address-based communication takes place with several devices downstream from the client. Clients with this setting cannot connect to standard Wi-Fi devices and access points with firmware V3.0 or older.

For further information, refer to Section 5.4.6.

MAC Mode

IP frames in the direction from the client to the access point always have the MAC address of the WLAN interface as the source MAC address. As a result, the ARP tables at the access point end always contain only the MAC address of the WLAN interface of the clients.

If there are further devices downstream from the client, the Auto Find 'Adopt MAC' option should not be enabled. In this case, the MAC address would be assigned indiscriminately to the first device that signals over Ethernet.

If there is only IP communication between the access point and the client, the default setting *AdoptOwnMAC* can be retained. If MAC address-based frames also need to be sent by devices downstream from the client, you will need to select the settings Adopt MAC manually, Autofind Adopt MAC or layer 2 tunneling. For further information, refer to Section 5.4.6.

MAC Address/IP Address Assignment

The client maintains a table with the assignment of MAC address and IP address to be able to send incoming IP frames to the correct MAC address. The *IP Mapping Table* menu command display this table. In principle, any number of device is can be reached downstream from a client using IP. The client can manage up to eight devices. When a new device is added, the oldest entry is deleted from the table to make space is for the new entry. Since the data throughput of a wireless connection cannot be increased indefinitely, a maximum of the devices should be managed by one client.

6.6 The Filters Menu

Note

The *Filter* menu and the corresponding menu commands are available only available when you operate the SCALANCE W78x in the access point mode. You can specify the mode in the *System* menu.

6.6.1 MAC Filter Menu Command

If the MAC filter is activated, communication with clients on the Ethernet side is possible only when their source MAC addresses are entered in the table. As an alternative, it is possible to make a setting in which access is denied for all specified MAC addresses. You can enter a maximum of 50 MAC addresses in the table.

With IP mapping of a SCALANCE W78x in client mode, only the MAC address assigned to this device is relevant, the MAC addresses of the devices downstream from it on the Ethernet side are irrelevant for filtering.

Syntax of the Command Line Interface

CLI\BRIDGE\ MAC1FLT>

Command	Description	Comment
fltmac1 <E D>	Enables / disables the filter.	
statmac1 [F B]	If the value is set to F (forwarding), only packets with a source address contained in the table are forwarded. In mode B (blocking), these packets are blocked and all others are forwarded.	
add <MAC addr.> [description]	Adds a new address to the filter list. The optional description has no influence on the list and simply serves as information for the user.	
edit <Number MAC> [E D] [Description]	Changes the specified value.	
delete <Number MAC>	Deletes the entry from the list.	
clearall	Deletes all entries from the list.	

6.6.2 MAC Dir Filter Menu Command

Restriction of the Data Traffic between MAC Addresses

It is possible to filter the data traffic intended for wireless clients linked to the SCALANCE W78x access point. This filter is used to permit a specified MAC address access only to other specified MAC addresses. You can specify several source addresses or entries for one destination address. The communication of the destination address is then restricted to these entries. If a destination address is not entered in the filter, it is not subjected to any restrictions.

Syntax of the Command Line Interface

CLI\FILTERS\MAC2FLT>

Command	Description	Comment
fltmac2 <E D>	Enables / disables the MAC filter.	
add <SourceMAC> <DestMAC>	Adds a new entry with source and destination address to the filter.	
edit <Index> [E D] [SourceMAC] [DestMAC]	Changes the entry specified by <i>Index</i> . With [E D], you can enable / disable the entry.	
delete <Index>	Deletes the entry at the specified index position.	
clearall	Deletes all entries for the MAC filter.	

6.6.3 Protocol Filter Menu Command

Protocol Selection

Without protocol filtering, the SCALANCE W78x processes all data packets regardless of the protocol being used. To increase data security and to reduce load, it can nevertheless be useful to prevent communication using certain protocols.

Here, you are not restricted to the protocols included in the list in this menu. If necessary, you can add your own entries to this list. You can specify a maximum of 50 Ethernet II protocols for which filtering is required.

Syntax of the Command Line Interface

CLI\FILTERS\PROTO>

Command	Description	Comment
clearall	Deletes all entries for the protocol filter.	
statprot <F B>	The selected protocols are forwarded / not forwarded.	
fltprot <E D>	Enables / disables the protocol filter.	
add <pattern> [description]	Adds a new entry. A value in hexadecimal is expected for the <i>Pattern</i> value. The user can enter a short note for this protocol as the description.	
edit <index> [E D] [pattern] [description]	Changes of enables / disables the filter entry.	
delete <Index>	Deletes the filter entry.	
clearall	Deletes all entries from the table.	

6.7 The I-Features Menu

Note

The *I-Features* menu and the corresponding menu commands are available only available when you operate the SCALANCE W78x in access point mode. You can specify the mode in the *System* menu.

6.7.1 iQoS Menu Command

Note

This function is not available in iPCF mode.

Client-Specific Bandwidth Reservation

iQoS (Quality of Service) is technique with which clients are assigned a certain bandwidth. Due to this assignment, there is a high probability that data transmission to these clients will be within a defined period. This technique can be useful when response times must be guaranteed. If non-iQoS-clients put too much load on the network, they can be logged off from the AP to guarantee data traffic for iQoS clients.

Note

To ensure problem-free functioning of the iQoS mode, the number of clients with bandwidth reservation is restricted to four.

Note

If the user reserves data for critical clients, this data rate also includes the frame header (in other words, 802.11, MAC, IP, TCP, and S7 header). A SIMATIC user must therefore take into account not only the net data during configuration but also the headers.

Response Time

In the *Response Time* text box, you enter the required response time of the SCALANCE W78x over the wireless interface. Remember that this value represents the transmission time for the data from the SCALANCE W78x to the client. The data transmission rate for nodes not included in the list is reduced according the values specified.

Syntax of the Command Line Interface

CL\FEATURES\IQOS\WLAN1>

or for the second wireless adapter (if it exists)

CL\FEATURES\IQOS\WLAN2>

Command	Description	Comment
iqos [E D]	Enables / disables iQOS functionality.	
static [E D]	Enables / disables the calculation of the minimum transmission rate.	
response [<i>response time</i>]	Specifies the response time for a client with bandwidth reservation.	15 – 1000 ms, default 50 ms
add <MAC> <Max_BW> <E D>	Creating a critical client.	
edit <index> <Max_BW> <E D>	Changes the setting of a client	
delete <Index>	Deletes a critical client	
clearall	Deletes all critical clients	

6.7.2 iPCF Menu Command

Note

The iPCF menu command is available for a SCALANCE W788-xRR or SCALANCE W747-1RR and the IWLAN/PB Link.

Notice

With the SCALANCE W788-2RR, iPCF may only be enabled for one of the two WLAN interfaces.

Restrictions of the 802.11 Standard

With wireless LAN complying with IEEE 802.11, the maximum data throughput cannot be achieved in a cell when there is a higher number of nodes due to the resulting collisions. A further restriction are the handover times that can be achieved with 802.11 standard mechanisms. With normal commercially available WLAN products, these are of the order of several hundred milliseconds.

New Possibilities with iPCF

In an industrial environment, there are applications that require a deterministic response when there are large numbers of nodes and a high data throughput in a cell. A deterministic behavior is also required when changing cells with handover times of under 100 milliseconds.

To meet these requirements, the iPCF expansion (Industrial Point Coordination Function) was developed. iPCF is available with the following products:

- SCALANCE W788-1RR and SCALANCE W788-2RR
- SCALANCE W747-1RR
- IWLAN/PB Link

iPCF ensures that the entire data traffic of a cell is ordered, controlled by the access point. By avoiding collisions, the throughput can be optimized even with large numbers of nodes. iPCF also allows fast cell changes.

Note

For PNIO communication, we always recommend that you enable the iPCF mode. The signal strength must not fall below 60% or -65 dBm for reliable operation.

How iPCF Works

The basic principle of iPCF is that the access point scans all nodes in the cell cyclically. The same time, the scan includes the downlink traffic for this node. In the reply, the node sends the uplink data. The access point scans a new node at the latest every 5 ms.

The scan of a node can be seen by all other nodes in the cell. This allows a client to detect the quality of the link to the access point even when it is not communicating with the access point itself. If it does not receive a frame from the access point for a certain time, it starts to search for a new access point.

In iPCF mode, both the search for a new access point and the registration with this new access point have been optimized in terms of time. Handover times significantly below 50 ms are achieved.

When should iPCF be used?

iPCF can be recommended in particular when a high data throughput is required despite a large number of nodes or when extremely short handover times are required.

With PNIO data traffic (**ProfiNET IO**), the iPCF mechanism was further optimized by handling PNIO traffic with high priority.

What restrictions result from using iPCF?

The iPCF mechanism is a development of Siemens AG and the functions only with nodes on which iPCF is implemented. With an access point with two WLAN interfaces, it is, however, possible to set both iPCF and standard WLAN at the same time. iPCF was optimized for the use of RCoax cable and the access point and achieves optimum performance only with this configuration.

Configuration

Select the *iPCF Enabled* check box to enable the iPCF mode.

With the SCALANCE W788-xRR models, you can also set optimized support of PNIO if you select the *PNIO support enabled* check box. In this case, you must also set the *PNIO update time*. The PNIO update time must match the configured PNIO update time.

PNIO update times

When setting the update time, make sure that you note the following situations otherwise there is a risk that you will not be able to establish stable communication:

Case a: Your system operates in a single cell; in other words the clients (IWLAN/PB links, SCALANCE W74x) do not need to support roaming to another cell.

In this case, update times ≥ 8 ms are supported.

Case b: Your system operates with two cells on two different channels.

In this case, update times ≥ 16 ms are supported.

Case c: Your system operates with several cells and with more than 2 channels and the clients roam between cells.

In this case, the PN IO update time should be set higher than 16 ms.

Notice

We strongly advise that you check the local wireless characteristics prior to commissioning.

Syntax of the Command Line Interface

CL\FEATURES\IPCF\WLAN1>

or for the second wireless adapter (if it exists)

CL\FEATURES\IPCF\WLAN2>

Command	Description	Comment
ipcf [E D]	Enables or disables iPCF mode.	
pnio [E D]	Enables or disables optimized PNIO support.	Only on SCALANCE W788-xRR models (access point).
update <i>[time]</i>	Specifies the PNIO update time for cyclic PNIO data exchange. This value must match the configured PNIO cycle time.	Only on SCALANCE W788-xRR models (access point).

6.7.3 Forced Roaming on IP Down

Functional Description

Forced Roaming on IP down monitors the connection to a specific IP address cyclically. This is achieved using ICMP packets (Echo Request/Reply or Ping). If the IP connection aborts; in other words, no ping reply from the other end, a deauthentication frame is sent to all WLAN clients. The relevant WLAN interface is then disabled.

The IP connection continues to be monitored and the WLAN interface is enabled again as soon as the access point has received a ping reply from the pinged station.

The mechanism makes it possible, for example, to monitor a connection between wireless clients and a server. If the server can no longer be reached over the access point, the clients are deauthenticated and the WLAN interface of the access point is disabled. The clients roam and then connect to a different access point from which the server can be reached. As soon as the first access point can reach the server again, it re-enables its WLAN interfaces.

Syntax of the Command Line Interface

CLNFEATURES\FORCED_ROAM\WLAN1>

or for the second wireless adapter (if it exists)

CLNFEATURES\FORCED_ROAM\WLAN2>

Command	Description	Comment
froam [E D]	Enables or disables forced roaming on IP down.	
ip [IP address]	Monitors the connection to this IP partner.	
interval [100 - 5000]	Specifies the monitoring cycles to the IP partner in milliseconds.	
lostpkts [1 - 5]	Specifies the maximum number of unanswered pings before the WLAN interface is disabled.	

Note

Forced roaming on IP Down cannot be used in conjunction with iPCF or WDS on the same WLAN interface.

6.7.4 Link Check Menu Command

Note

This function is not available in iPCF mode.

Device-Related Connection Monitoring

The Link Check function provides device-related connection monitoring for a maximum of ten wireless nodes logged on at the SCALANCE W78x. This service can be compared with the link on a wired connection. The function monitors whether the node is available over the wireless medium. If no packet is received from the node or sent successfully after half of the configured monitoring time, the SCALANCE W78x attempts to send a test packet to the node.

Note

With the Link Check function, you can only monitor connections to WLAN clients; use along with redundancy or WDS is not possible.

System Event for Connection Abort

You can specify how the SCALANCE W78x reacts to a connection abort (or to the reestablishment of a connection) in the *System > Events* menu.

Syntax of the Command Line Interface

CLINFEATURES\LINKCHECK>

Command	Description	Comment
linkchk [E D]	Enable / disable device-related connection monitoring.	
add <MAC> [timeout]	Adds a new MAC address for connection monitoring and specifies the monitoring time. No time is specified, the default is 500 ms.	
edit <Index MAC> [E D] [timeout]	Modifies, enables, or disables an entry.	
delete <Index MAC>	Deletes the specified entry from the list.	
clearall	Deletes all entries for connection monitoring.	
acknow [Index all]	Displays or acknowledges (clears) the Link Check messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. Default status and the LED are cleared if the reason for default status was <i>only</i> a link check error message.

6.7.5 Redundancy Menu Command

Note

The redundancy function described here is available only with SCALANCE W78x models that have two wireless adapters available (SCALANCE W788-2PRO and SCALANCE W788-2RR) and that are not operating in iPCF mode.

You can only use the encryption schemes **WEP** and **AES**.

Redundant Connection between two SCALANCE W788-2xx Devices

Note

With the firmware update to \geq V3.0, the SCALANCE W78x-xRR devices need to be reconfigured if you use WDS or redundancy and use the MAC address and not the system name (sysName).

These functions are then based on the MAC address that changed with the introduction of VAPs with V3.0.

Two SCALANCE W78x devices each with two wireless interfaces can be configured so that there is a redundant wireless connection. The redundancy function causes an automatic failover to the second wireless interface if no data transfer is possible on the first wireless interface. The user is informed of the status of the redundant connection with the statuses *not connected*, *connected*, or *error* (communication error).

Instead of the MAC addresses, you can also configure the redundant partners with the sysName parameter. Beacons contain this parameter which is why the redundant device is detected using beacons.

Note

If 802.1x or WPA is used, a *private key* must be selected for the redundant connection.

Syntax of the Command Line Interface

CLIN\FEATURES\REDUNDANCY>

Command	Description	Comment
redun [E D]	Enables / disables the redundancy function	
wep [E D]	Enables / disables encryption.	
mac1 <MAC address>	Specifies the device that will be operated redundantly along with the first wireless adapter.	
mac2 <MAC address>	Specifies the device that will be operated redundantly along with the second wireless adapter.	
name [system name]	Instead of the MAC addresses, you can also specify the sysName of the device.	
wepkey1 [key index]	Specifies the WEP key of the device that will be operated redundantly along with the first wireless adapter.	
wepkey2 [key index]	Specifies the WEP key of the device that will be operated redundantly along with the second wireless adapter.	

6.7.6 IP-Alive Menu Command

Application-Related Connection Monitoring

The IP-Alive function provides application-related connection monitoring of the wireless link.

It is useful to use IP-Alive on IP connections when it is known that they are used to send data cyclically. With IP-Alive, you specify a monitoring time for an IP address and a port. If you do not want to monitor a particular port but rather only the data traffic from a particular IP address, simply enter 0 in Port. This resets the monitoring with each frame from this IP address.

In contrast to the Link Check, the SCALANCE W78x does not start any checks until the monitoring time has elapsed. The SCALANCE W78x checks passively whether communication took place during the specified monitoring period. As with Link Check, you can also enter up to ten connections here.

System Event for Connection Abort

You can specify how the SCALANCE W78x reacts to change in the IP-Alive status in the *System > Events* menu.

Note

The IP-Alive function is not available in iPCF mode.

Syntax of the Command Line Interface

CLINFEATURES\IP_ALIVE>

Command	Description	Comment
ipalive <E D>	Enables / disables application-related connection monitoring.	
add <E D> <IP address> <:Port> <Timeout>	Adds a new IP address to the connection monitoring and enables / disables monitoring for this IP address.	
edit <index IP addr.> [:port] [E D] [timeout]	Modifies, enables, or disables the entry specified by the index or IP address.	
delete <Index IP addr.>	Deletes the node to be monitored.	
clearall	Deletes all entries for connection monitoring.	
acknow [Index all]	Displays or acknowledges (clears) the IP Alive messages requiring acknowledgment.	The fault state remains active until all the fault messages have been acknowledged. The fault state and the Fault LED are cleared if the only reason was an IP Alive error message. The command is not visible in the client mode.

6.8 The Information Menu

System Events and Information on the Protocols

The pages of this menu display tables contain information on system events and on the behavior of the protocols (IP, TCP, UDP, and ICMP, SNMP).

Updating the Display

Most pages have the *Refresh* button at the bottom edge with which you can update the display. The *Client List* menu command also allows you to update automatically. To activate this, select the *Update* check box.

Syntax of the Command Line Interface

CLI\ ... >

Command	Description	Comment
info	Displays information on the current menu item.	This can be called in every submenu.

6.8.1 Log Table Menu Command

Logging System Events

This page lists system events and the time at which they occurred. You can specify which events are included here in the *System > Events* menu.

If you position the mouse pointer over a time value, the system time and date are displayed.

Syntax of the Command Line Interface

CL\INFORM\LOG>

Command	Description	Comment
events <show clear>	Displays or deletes the log table.	
addevent <Text>	Adds an event to the log table.	
eventmax [Max count]	Sets the maximum number of log entries.	The default is 400.

6.8.2 Auth Log Menu Command

Logging Authentication

The pages of this menu contain a table with information on successful or failed authentication attempts.

Syntax of the Command Line Interface

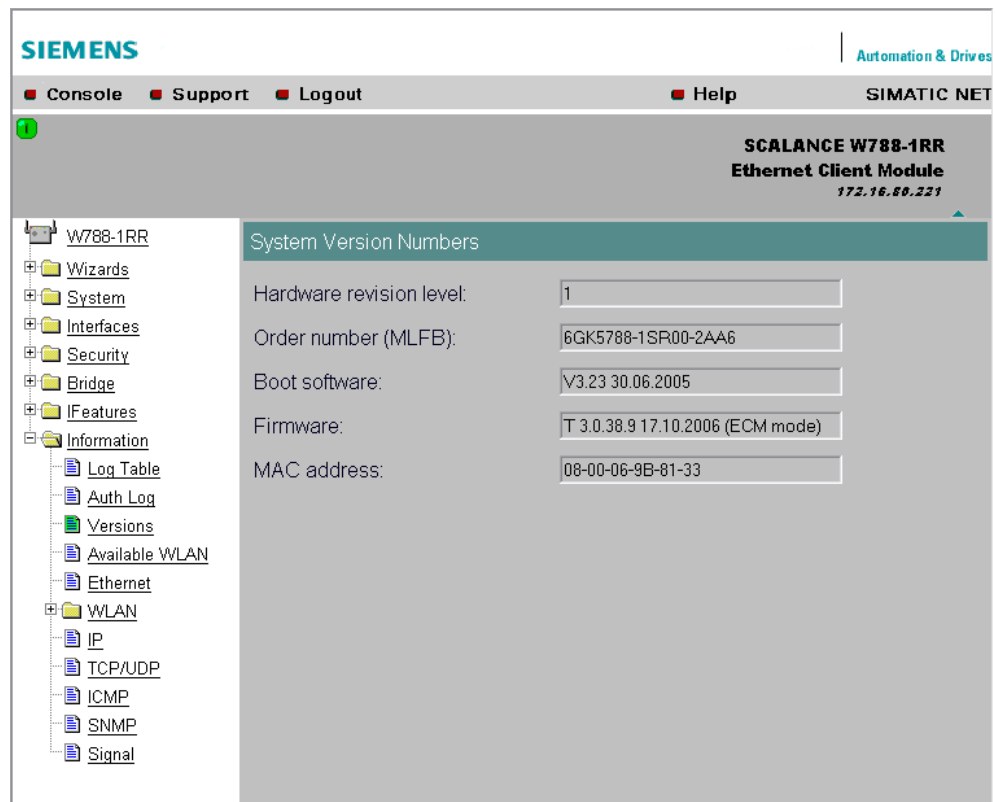
CLI\INFORM\LOG>

Command	Description	Comment
show [0...8]	Displays the authentication entries. By specifying a parameter, the display can be limited to specific information: 0 All 1 Good 2 All errors 3 802.11 errors 4 ACL errors 5 RADIUS errors (request denied, password denied etc.) 6 802.1x errors (timeout, no response from RADIUS or WPA server) 7 Deauthenticated errors 8 Deassociated errors	
clear	Deletes all entries.	

6.8.3 Versions Menu Command

Current Versions and Order Numbers

1. Hardware version
2. Order number (MLFB)
3. Boot software version
4. Firmware version
5. Ethernet MAC address



6.8.4 Client List Menu Command

Note

This menu command is available only in the access point mode.

Logged on Clients

All the clients logged on at the SCALANCE W78x along with certain additional information (wireless channel, status etc.) are displayed here.

MAC address

The MAC address of the client.

If#

This specifies the wireless interface over which the client is connected.

Signal

The signal strength of the client. The higher the value, the better the signal. The user can choose between percentage and dBm.

Age

Displays the time that has elapsed since the last client activity was detected.

Sec

This indicates which encryption is active.

Channel.

The current channel over which the client communicates with the SCALANCE W78x.

State

The current state of the clients. *Associated* means that the client is logged on.

SIEMENS Automation & Drives

Console **Support** **Logout** **Help** **SIMATIC NET**

SCALANCE W788-2RR
Dual Access Point
172.16.88.221

W788-2RR

- Wizards
- System
- Interfaces
- Security
- Bridge
- Filters
- IFeatures
- Information
 - Log Table
 - Auth Log
 - Versions
 - Clients list
 - Ethernet
 - WLAN 1
 - WLAN 2
 - iQoS
 - Spanning Tree
 - IP
 - TCP/UDP
 - ICMP
 - SNMP

Associated Stations (22) Unit **dBm** Update ☐

Type	MAC address	If#	Signal	Age	Sec	Ch.	State
Sta	08-00-06-94-3E-4E	1	-39 dBm	< 1 s	x	153	Associated
Sta	08-00-06-96-A2-E0	1	-31 dBm	4 s	x	153	Associated
WDS	08-00-06-97-B6-20	2	-30 dBm	< 1 s	x	157	AP is up
WDS	08-00-06-97-B9-58	2	-44 dBm	< 1 s	x	157	AP is up
WDS	08-00-06-97-EE-B0	2	-43 dBm	< 1 s	x	157	AP is up
WDS	08-00-06-97-ED-D8	2	-40 dBm	< 1 s	x	157	AP is up
WDS	08-00-06-9B-81-28	2	-47 dBm	< 1 s	x	157	AP is up
Sta	08-00-06-97-F3-1E	2	-42 dBm	4 s	x	157	Associated
Sta	08-00-06-97-B8-7C	2	-30 dBm	4 s	x	157	Associated
Sta	08-00-06-97-EF-22	2	-30 dBm	4 s	x	157	Associated
L2T	08-00-06-97-ED-42	2	-31 dBm	< 1 s	x	157	Associated
Sta	08-00-06-93-E8-0A	2	-52 dBm	< 1 s	x	157	Associated
Sta	08-00-06-70-18-B6	2	-30 dBm	< 1 s	x	157	Associated
Sta	08-00-06-93-E8-13	2	-38 dBm	< 1 s	x	157	Associated
Sta	08-00-06-97-ED-EA	2	-60 dBm	4 s	x	157	Associated

Refresh

By selecting the *Update* check box, the list is updated automatically every 2 seconds. If you click on the MAC address of a client, you will receive additional information on this client.

Syntax of the Command Line Interface

CLI\INFORM\WLAN1>

CLI\INFORM\WLAN2>

Command	Description	Comment
Station	Displays information on the connected stations.	
resetStats	Resets the statistics that are displayed with the <i>Station</i> command.	
Apinfo	Displays information on the access point.	(only in access point mode)
Scan	Displays all the access points in the area.	
Noise	Shows disturbances on the individual channels.	

6.8.5 Ethernet Menu Command

Information on the Ethernet Interfaces

This menu command provides information on the current settings of the Ethernet interface. The current operating data is also displayed here.

Syntax of the Command Line Interface

There are no CLI commands for this menu command.

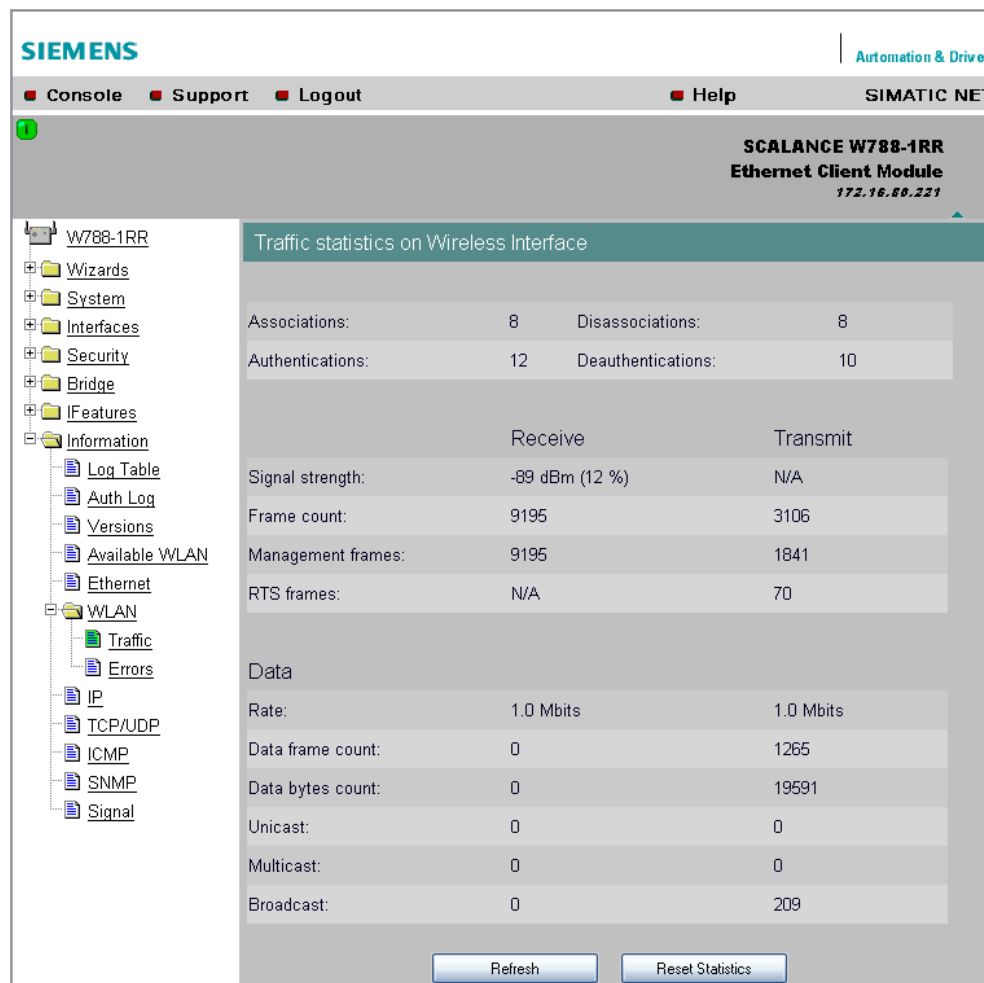
6.8.6 WLAN Menu Command

Information on the WLAN Interface

This menu command provides information on the current settings of the WLAN interface. The current operating data is also displayed here. With the SCALANCE W788-2PRO and SCALANCE W788-2RR models, there are two menu commands *WLAN1* and *WLAN2*.

Traffic

Statistics of the data to be transmitted are displayed here.



- **Association / Authentication Frames**

The frames relevant for registration are counted. A distinction is made between the registration frames Association and Authentication and the deregistration frames Disassociation and Deauthentication.

- **Signal strength**

The signal strength is displayed as an average of the last received frames or at the sending end of the last received Acknowledge frames.

- **Frame count**

Counter for all successfully received or sent frames.

- **Management frames**

Counts all received or sent management frames.

- **RTS frames**

Is incremented when a CTS frame is received in response to an RTS frame.

- **Rate**

Displays an average data rate of the most recently received or sent data frames.

- **Data frame count**
Counts all received or sent data packets.
- **Data bytes count**
Displays the sum of all received or sent bytes in a data frame.
- **Unicast**
Sum of all received or sent data unicasts.
- **Multicast**
Sum of all received or sent data multicasts.
- **Broadcast**
Sum of all received or sent data broadcasts.

Errors

This page displays statistics of the transmission errors that have occurred. A high error rate indicates a bad connection.

SIEMENS | Automation & Drives

Console Support Logout Help SIMATIC NET

SCALANCE W788-1RR
Ethernet Client Module
172.16.80.221

W788-1RR

- Wizards
- System
- Interfaces
- Security
- Bridge
- IFeatures
- Information
 - Log Table
 - Auth Log
 - Versions
 - Available WLAN
 - Ethernet
 - WLAN
 - Traffic
 - Errors
 - IP
 - TCP/UDP
 - ICMP
 - SNMP

Error statistics on Wireless Interface Update

Receive		Transmit	
ACL discarded frames:	0 (0 %)	Transmission errors:	226 (6 %)
Fragmentation errors:	0 (0 %)	Dropped frames:	42 (1 %)
Encryption errors:	0 (0 %)	ACK errors:	5076 (0 %)
Duplicate frames:	7 (0 %)	RTS errors:	550 (88 %)
FCS errors:	1338 (13 %)	Retry count:	778 (21 %)
Header CRC errors:	1098 (11 %)	One retry count:	729 (20 %)
Decrypt CRC errors:	0 (0 %)	Multiple retry count:	49 (1 %)

Refresh Reset Statistics

Receive Errors:

- **ACL discarded frames**
Displays all client registration attempts that were blocked by the Access Control List.

- **Fragmentation errors**
Sum of all failed fragmentations. One of the fragments was not received or received too late.
- **Encryption errors**
Is incremented if a frame is received in which the WEP bit is set and the device operates without encryption, or the reverse situation when a packet is received without a WEP bit and encryption is enabled.
- **Duplicate frames**
Sum of all frames received twice.
- **FCS errors**
Sum of all packets received in which the checksum was incorrect.
- **Header CRC error**
Sum of all packets received in which the header checksum was incorrect.
- **Decrypt CRC error**
Sum of all packets received in which the checksum of the encrypted data buffer was incorrect.

Transmit Errors

- **Transmission errors**
Is incremented when a frame cannot be sent successfully despite hardware retries.
- **Dropped frames**
Number of packages that were dropped either when the packet was not sent despite all retries or packets that had not been sent when a node deregistered.
- **Acknowledged errors**
Sum of all packets sent that were not confirmed by an acknowledge.
- **RTS errors**
Sum of all sent RTS frames that were not acknowledged by a CTS.
- **Retry count**
Sum of all frames sent successfully that required one or more retries.
- **One retry count**
Sum of all frames sent successfully that required exactly one retry.
- **Multiple retry count**
Sum of all frames sent successfully that required more than one retry.

Note

The percentages shown following the errors relate to the entire received/sent frames.

Overlap AP

Note

This menu command is available only in the access point mode.

For optimum data throughput, it is important that the set wireless channel is not used by other access points. In the 2.4 GHz band (802.11b or 802.11g), there is overlapping of the wireless channels so that an access point occupies not only the set channel but also the two or three adjacent channels. You should therefore make sure that there is adequate channel spacing to neighboring access points.

The *Overlap AP* page shows all access points that are visible on the set or adjacent channels (at 2.4 GHz). If entries exist here, the maximum data throughput of the access point will be restricted.

Type

Shows the type of connection. The types AP (infrastructure mode) and AdHoc exist.

MAC address

The MAC address of the wireless devices.

Channel

The channel on which the found wireless device transmits.

Signal

Shows the signal strength with which the other wireless devices are received at the AP. The stronger the signal, the greater the probability that they interfere with each other. There is also the possibility that they interfere with each other even at low signal strengths.

Age

Shows when the last activity was detected by the wireless device.

SSID

Shows the SSID of the other wireless device.

Syntax of the Command Line Interface

CL\INFORM\WLAN1>

or for the second wireless adapter (if it exists)

CL\INFORM\WLAN2>

Command	Description	Comment
overlap	Shows the access points on the set or adjacent channels.	
over_age [1..7200]	Changes the aging interval (in minutes) for the list of neighboring access points. If an AP is inactive for longer than the time set here, it is removed from the list.	

VLAN

This page displays information on the configured virtual LANs with the following information on each virtual access point (VAP):

- *Port Name*
The configured port name. Here, you see a list of the configured virtual access points (VAP), the WDS connections and the management and the redundancy VLAN if applicable.
- *VLAN*
The status of the relevant VLAN (E = enabled, D = disabled)
- *VLAN ID*
The configured VLAN ID
- *SSID*
The SSID of the relevant VLAN
- *Member*
Shows the virtual access point (VAP) as member of other VLANs:
all = VAP is member of all VLANs
only = VAP is member of only certain VLANs
- *Priority*
The configured frame prioritization

6.8.7 iQoS Menu Command

Information on Bandwidth Reservation

The pages of this menu provide information on iQoS. The clients are grouped as follows:

Critical Compliant (CC)

This involves clients that were defined as critical and that are currently meeting the requirements you set for the bandwidth and response time.

Critical Non-Compliant (CNC)

The CNC clients are also clients with strict requirements regarding the response time and bandwidth. In contrast to the CC clients, however, these clients are not currently meeting these requirements.

Non-Critical Satisfied (NCS)

These clients do not have fixed requirements regarding the response time and minimum bandwidth. Their communication is not currently restricted by iQoS.

Non-Critical Regulated (NCR)

These clients are also non-critical clients whose communication is, however, currently being restricted by iQoS in favor of critical clients.

Non-Critical Non-Responsive (NCNR)

Some clients that require no acknowledgment whatsoever for their communication (for example UDP traffic) cannot be regulated by iQoS. These are classified as *NCNR*.

Syntax of the Command Line Interface

CLINFEATURES\IQOS\WLAN1>

or for the second wireless adapter (if it exists)

CLINFEATURES\IQOS\WLAN2>

Command	Description	Comment
info	Displays information on iQos.	

The CLI also supplies detailed information on iQoS. In this view, the first part displays the current configuration, in other words whether iQoS is enabled, , whether the calculations and reservations are based on the static worst-case assumptions (static = enabled) or the current situation (static = disabled). The number of configured critical clients is also displayed.

```

Telnet 192.168.1.9
CLI\IFEATURES\IQOS\WLAN1>info
iQoS : enabled
static : disabled
Guarantee Time : 50 ms
Critical Clients : 1
Index : MAC Address : Bandwidth (kbit/s) : Enabled : Accepted
-----
1 : 08-00-06-2A-BB-06 : 200 : X : X

Traffic statistics (Timestamp: 100016 ms):
      : CC : CNC : NCS : NCR : NCNR
-----
Number of clients : 1 : 0 : 3 : 0 : 0
Framerate : 193 : 0 : 470 : 0 : 0

Associated Clients:
AID : MAC Address : SI (ms) : Status : TX bytes : RX bytes
-----
4 : 00-0D-88-65-13-B1 : 1.62 : NCS : 241711 : 43041
3 : 00-05-5D-9A-13-FF : 1.62 : NCS : 10049620 : 10063453
2 : 08-00-06-2A-BB-06 : 0.0 : CC : 509256 : 512666
1 : 00-50-8B-5E-0B-DB : 1.62 : NCS : 557405 : 566839

SI = shaper interval
CC = critical compliant
CNC = critical non-compliant
NCS = non-critical satisfied
NCR = non-critical regulatedNCR
NCNR = non-critical non-responsive
CLI\IFEATURES\IQOS\WLAN1>

```

The *Traffic statistics* table shows how many clients are currently in each status and how many packets of a particular class were sent for each of these classes.

The *Associated Clients* table provides an overview of all clients, their current classification, and the volume of sent and receive data. The shaper interval (SI) is also displayed for each client. The shaper interval is the minimum spacing between two packets of a client set by iQoS. For NCS clients, the SI is selected so that their bandwidth is twice the size of the current bandwidth.

6.8.8 Spanning Tree Menu Command

Status of the Spanning Tree Protocol

The upper part of the page shows the *RootID* and the *BridgeID*. Both IDs are made up of their priority and their MAC address. Together, this results in the 16 character long ID. The RootID is the ID of the bridge that is currently the root bridge. The BridgeID shows the ID of the local device.

Below this, you can see values for the Topology Change event. The first value is a counter indicating how often the tree structure has changed since restarting. The value beside this, shows the time since the last switchover event.

SIEMENS | Automation & Drives

Console Support Logout Help SIMATIC NET

SCALANCE W788-1RR
Access Point
172.16.80.221

(Rapid) Spanning Tree Protocol Status

Version: RSTP
 RootID: 0000000000000000 BridgeID: 80000800069b8133
 Root priority: 0 (0x0000) Bridge priority: 32768 (0x8000)
 Root MAC: 00-00-00-00-00-00 Bridge MAC: 08-00-06-9B-81-33
 Topology changes: 0 Time since topology change: 0 days, 0:00:00

Port Name	En	Cost	Priority	Edge	P.t.P.	Port State	State
Ethernet	X	100	128	X	-	FORWARDING	BLOCKED
WLAN 1	X	33	128	X	-	FORWARDING	BLOCKED
WLAN 1 VAP 1	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 VAP 2	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 VAP 3	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 VAP 4	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 VAP 5	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 VAP 6	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 VAP 7	-	100	128	X	-	DISCARDING	BLOCKED
WLAN 1 WDS 1	-	100	128	-	-	DISCARDING	BLOCKED
WLAN 1 WDS 2	-	100	128	-	-	DISCARDING	BLOCKED
WLAN 1 WDS 3	-	100	128	-	-	DISCARDING	BLOCKED
WLAN 1 WDS 4	-	100	128	-	-	DISCARDING	BLOCKED
WLAN 1 WDS 5	-	100	128	-	-	DISCARDING	BLOCKED

Refresh

Below this, you will see the following port-related information:

Port Name

Plain language name of the port, for example Ethernet or WLAN1 WDS1.

Enabled

Indicates whether the (R)STP is enabled for this port. If the port is not enabled, no further frames are forwarded over this port.

Cost

Indicates the path costs for the port.

Priority

Indicates the current priority of the port.

Edge

Shows whether or not the port is an edge port.

P.t.P.

Shows whether or not the AP is connected directly to another (R)STP device

Port State

With STP, a port can adopt three states:

- **Discarding**
No frames are forwarded from or to this port. The port has been disabled by the user or the protocol (for example, when a redundant path has been detected).
- **Learning**
The port receives packets in the same way as in listening mode, but does not forward them. The MAC addresses are also entered in the *Learning Bridge*.
- **Forwarding**
The port is fully enabled. Frames can be received and sent.
- **Disabled**
The port is not currently in use.

State

Here, the state of the port in relation to the root bridge is displayed. The *ROOT* state means that the port is connected directly with the root bridge. *DESIGNATED* identifies all ports that are not directly at the root but that are enabled. Ports that are blocked are in the *BLOCKED* state.

Syntax of the Command Line Interface

The Command Line Interface contains the information on the Spanning Tree protocol in `CLI\INFORM\Spanning`.

6.8.9 IP, TCP/IP, ICMP, SNMP Menu Command

Information on Protocols

The pages of this menu show information on the IP, TCP, UDP, ICMP, and SNMP protocols in the form of tables.

There are no CLI commands for this menu command.

6.8.10 Signal Recorder Menu Command

Note

The signal recorder is available only in client mode.

Signal Strength Indicators

The Signal Recorder can record or display the signal strength of the connected access point. Using this data, you can locate areas with an inadequate signal strength. The Signal Recorder can be particularly advantageous when the client moves along a fixed path (for example suspension track).

Using the URL

http://<IP address>/Signal.txt

or the URL

http://<IP address>/Signal.log

you can download the generated Signal file. If you are not yet logged in, this opens the login window in which you must log in with the Admin login.

Displaying the Instantaneous Value

The upper half of the window contains an instrument for displaying the graphic representation of the currently calculated dBm value in real time. Depending on your browser and the network load, the display is updated approximately every 500 ms. Apart from the graphic display, the current dBm value is also displayed in plain language. The MAC address of the AP with which the ECM is currently connected along with the frequency, channel and transmission rate are also displayed and updated. You can start or stop the graphic display with the "Start display" and "Stop display" buttons.

Note

Working with the graphic display can cause a not insignificant network load that can disturb time- and throughput-critical processes (iPCF, PNIO).

Recording a Series of Measurements

The lower half of the window includes not only the operator controls for graphic display of the instantaneous value but also the controls for the actual signal recorder. You can set the interval between the acquisition of two measuring points as well as the total number of measuring points. The recorder is controlled by the "Start recording" and "Stop recording" buttons.

As soon as measuring points have been recorded successfully and the recorder has been stopped, the "Save recorder file" and "Display recorder file" buttons are enabled. With the "Save" button, the measured values can be loaded directly from the ECM as a file in CSV format and imported into a suitable evaluation program.

The CSV file contains the MAC address of the AP for every measuring point, the current number of the measurement, the raw value of the RSSI, the dBm value and its corresponding percentage value, a roaming indicator, the channel and the transmission rate.

The "Display record file" button opens a pop-up window in which the measured values over time is already available in graphic form. The dBm values are shown over time. If the ECM roams during the measurement, blue bars indicate the event. If you move the mouse pointer over such a bar or over the flag at the top of the bar, a tooltip with the MAC addresses of the two access points appears.

With the "Print graph" button, it is easy to print the table. You will, however, need to make certain settings in the browser.

- Mozilla Firefox 1.5:
In the "File" => "Page setup..." dialog, make sure that the "Print Background (colors & images)" check box is enabled in the "Options" group box.
- Microsoft Internet Explorer 6.0:
In "Tools" => "Internet Options" => "Advanced", the "Print background colors and images" check box must be enabled under "Printing".

The signal recorder itself does not cause any significant load in the network that could affect other processes.

Both parts of the signal recorder can be operated independently.

Below, you will find a few tips that will help you to obtain useful measurements with the signal recorder:

- Use a fixed data rate in the configuration.
- Where possible, the ipcf mode with as low an update time as possible should be set for the measurements.
- Make sure that there is enough data communication during the measurement because the statistics functions evaluate incoming frames.
- The measurement setup should be run through 2-3 times with the same parameters to find out whether losses of signal strength always occur at the same position.
- Selective measurements at a fixed position should be made over a certain time.

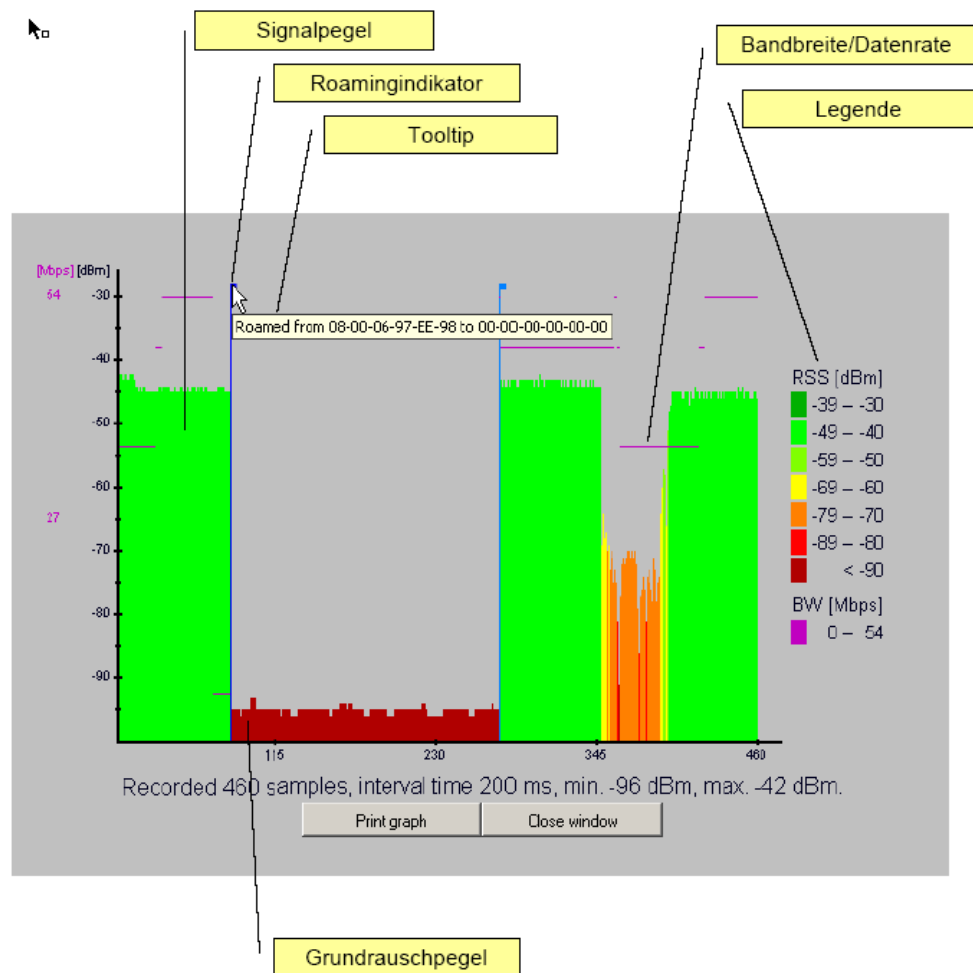


Figure 6-3 Screen Display of the Measured Values

Roaming indicator

This value appears when the client connects to another or to no AP and the MAC address of the AP changes as a result.

Bandwidth/data rate

The bandwidth/data rate is not displayed over the entire screen since it could overlap the signal level.

Noise floor

The noise floor represents the lower end of the technically possible transmission of the device. This means that when the noise floor is exceeded (the useful signal is louder than the noise floor), this is where the system dynamics begins. For this reason, this level is visible only when the client has no connection to an AP (indicated in the figure above by the MAC address 00-00-00-00-00-00).

Legend

BW bandwidth in Mbps

RSS received signal strength in dBm

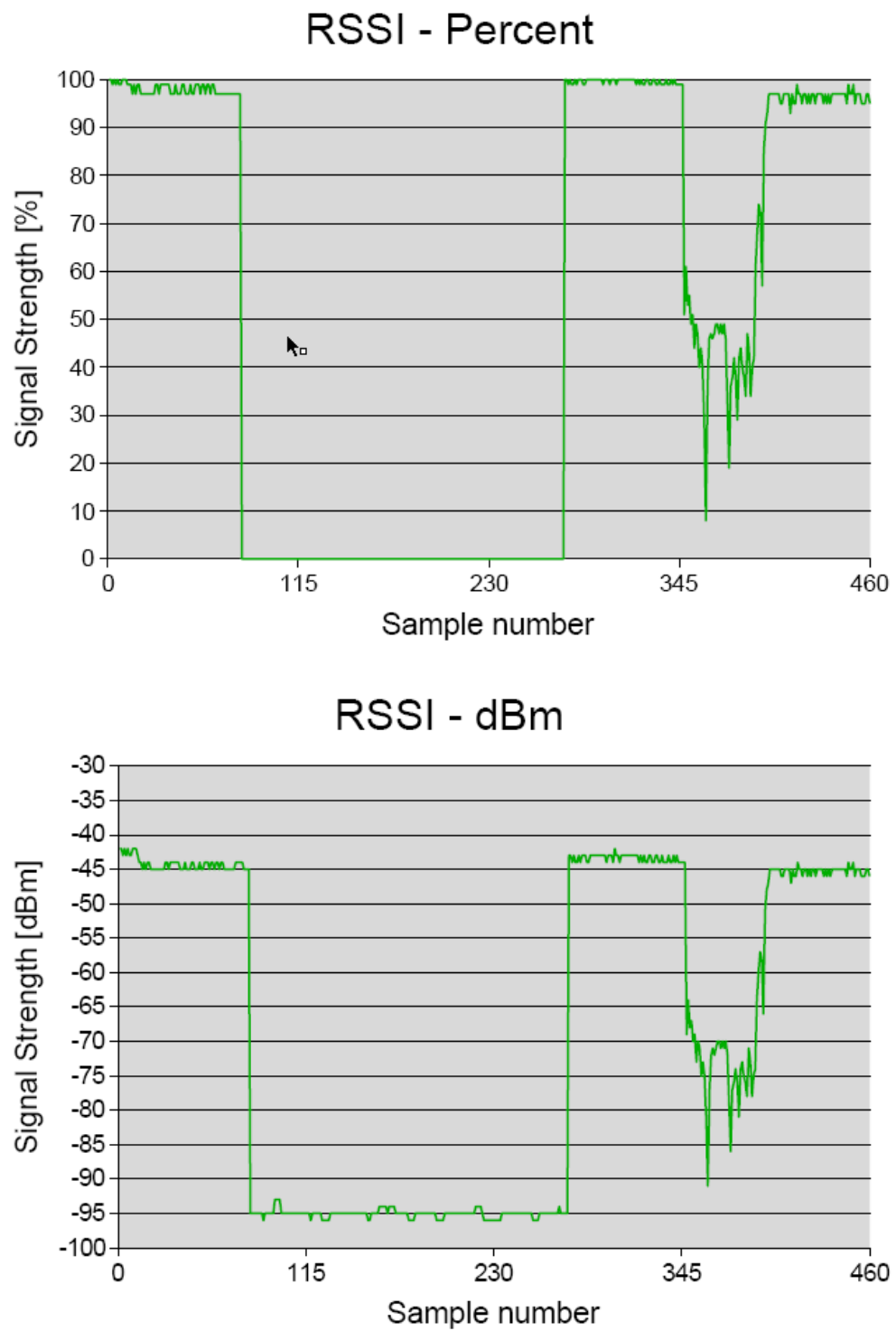


Figure 6-4 Comparison of the Measured Value Display as a Percentage and in dBm

Syntax of the Command Line Interface

CLI\INFORM\SIGNAL>

Command	Description	Comment
restart <interval> [quantity recording points]	Starts signal recording. The interval at which the current signal is recorded can be between 1 and 1000 milliseconds. A value between 1 and 20000 is possible for the number of recording points.	This command is only available in the client mode.
recstop	Stops signal recording prematurely.	This command is only available in the client mode.
dispstart [interval]	Displays the current signal strength cyclically on the CLI. The interval can be between 100 and 10000 milliseconds	This command is only available in the client mode.
dispstop	Stars cyclic output of the signal strength.	This command is only available in the client mode.
exit	Closes the CLI/TELNET connection.	This command is only available in client mode
info	Displays the parameters of the signal recorder	This command is only available in client mode

Technical Specifications / Approvals

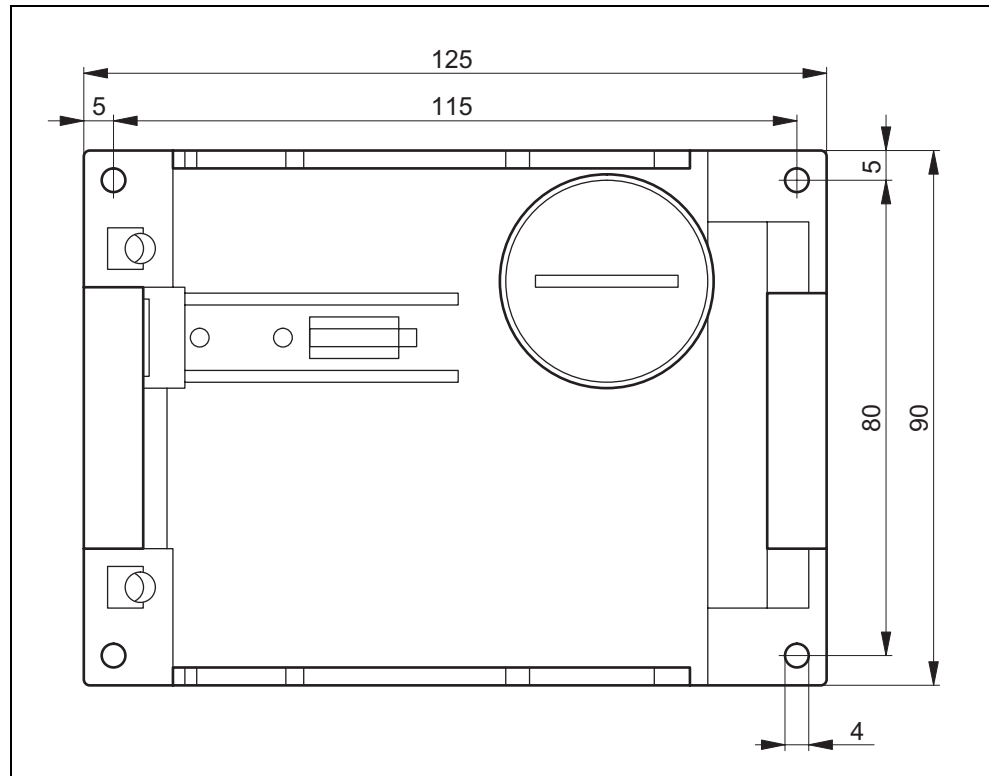
7

Data Transmission	
Transmission rate for Ethernet	10/100 Mbps
Transmission rate for wireless	1 ... 54 Mbps (108 Mbps)
Supported standards for wireless	802.1x, 802.11a, 802.11b, 802.11g, 802.11h, 802.11i
Supported standards for energy supply	802.3 af (Power over Ethernet)
Interfaces	
Energy	<ul style="list-style-type: none"> • M12 connector (18 to 32 V DC) • Power contacts in the hybrid connector (18 to 32 V DC) • RJ-45 jack power-over-Ethernet (48 V DC) <p>2 DC 24V power supplies (18 to 32 V DC) safety extra-low voltage (SELV). Power supply voltage connected over high resistance with housing (not electrically isolated).</p>
Data	IE IP 67 hybrid plug-in connection R-SMA antenna sockets (2 x or 4 x with the 7882pro)
Electrical Data	
Power consumption	< 10 W
Construction	
Dimensions without antennas (W x H x L)	125 mm x 88 mm x 108 mm
Weight	approx. 1050 g
Permitted ambient conditions	
Operating temperature	-20°C ... 60°C
Transport and storage temperature	-40°C ... 70°C
Degree of protection	Tested to IP65

MTBF Information (mean time between failure)

Device type	MTBF
SCALANCE W78x	67 years

Drilling diagram for wall mounting



Technical Specifications ANT795-4MR

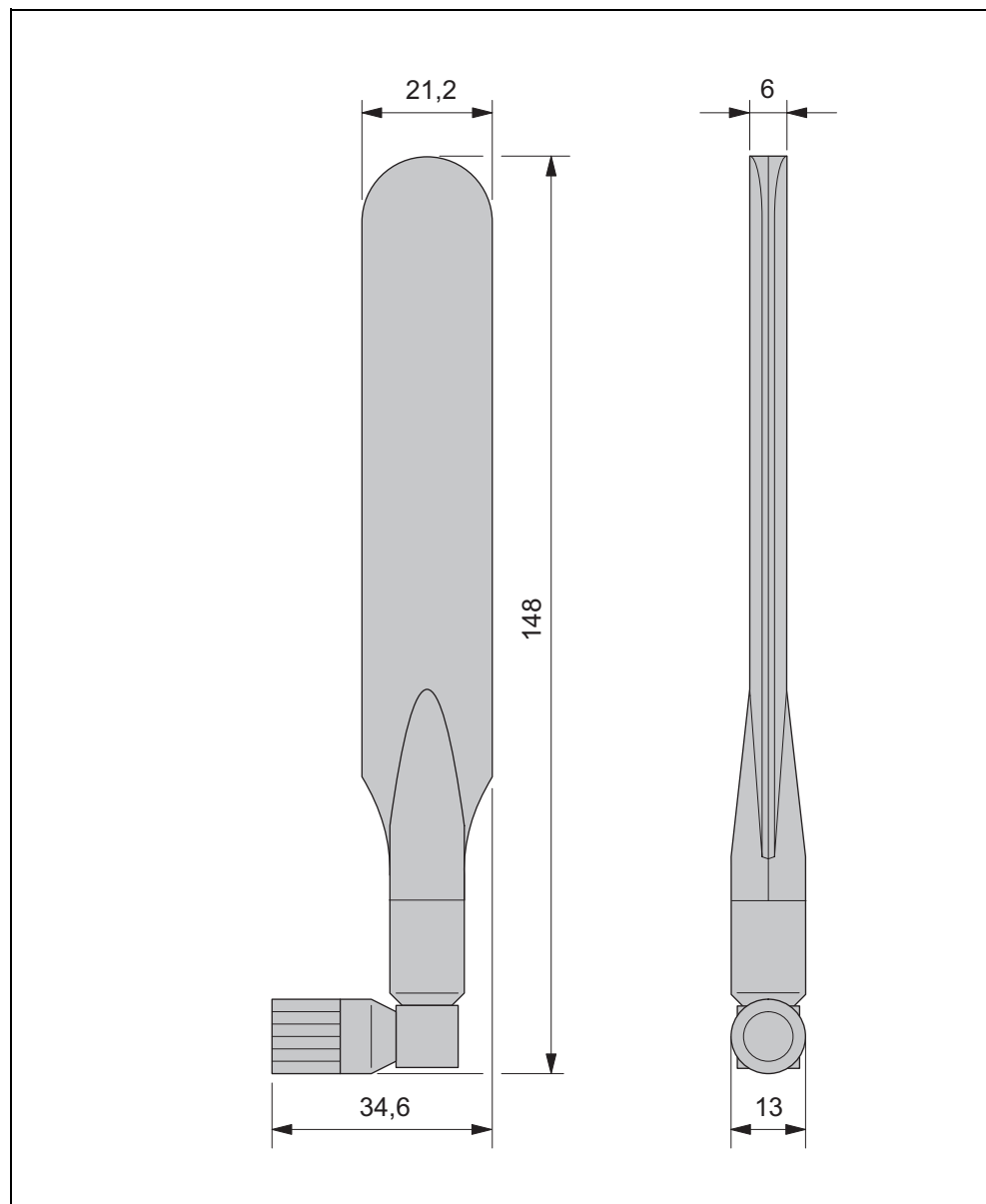
Mechanical Properties

Connector	R-SMA male for connection to SCALANCE W78x or SCALANCE W74x
Cover material	Polycarbonate
Silicone-free	

Electrical Properties

Frequency range	2.4 ~ 2.4835 GHz 5.15 ~ 5.35 GHz 5.725 ~ 5.85 GHz
Impedance	50 Ohms
Voltage standing wave ratio	$\leq 2,0$
Return loss	≤ -10 dB
Gain at 2.45 GHz	3 dBi
Gain at 5.25 GHz	5 dBi
Polarization	Vertical
Operating temperature	- 20 °C.... + 60 °C

Dimension Drawing



Approvals

CE Conformity

The products

SIMATIC NET SCALANCE W788-1PRO

SIMATIC NET SCALANCE W788-2PRO

SIMATIC NET SCALANCE W788-1RR

SIMATIC NET SCALANCE W788-2RR

in the version put into circulation by Siemens A&D conform to the regulations of the following European directive:

99/5/EC

Directive of the European Parliament and of the Council relating to Radio Equipment and Telecommunications Terminal Equipment and the Mutual Recognition of their Conformity.

Conformity with the essential requirements of the directive is attested by adherence to the following standards:

EN 60950

Safety of Information Technology Equipment

EN 301 489-1

Electromagnetic Compatibility for Radio Equipment and Services

EN 301 489-17

Specific Conditions for Wideband Transmission Systems and High-Performance Radio Local Area Network (HIPERLAN) Equipment

EN 300 328

Electromagnetic Compatibility and Radio Spectrum Matters

EN 301 893

Broadband Radio Access Networks (BRAN) - 5-GHz high-performance RLAN

EN 50371

Generic standard to demonstrate the compliance of low power electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)

1999/519/EC

Council recommendation on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz)

Devices connected to the system must meet the relevant safety regulations.

The EU declaration of conformity is available for the responsible authorities according to the above-mentioned EU directive at the following address:

Siemens Aktiengesellschaft
Automation and Drives
Industrielle Kommunikation
Postfach 4848
D-90327 Nürnberg

This declaration certifies compliance with the directives named above, but does not guarantee any specific properties.

Declaration of Conformity

Manufacturer / responsible person Dietmar Herian
 Address: Siemens AG
A&D PT 2
Östliche Rheinbrückenstr. 50
76187 Karlsruhe

Declares that the product:

type: Scalance W 700-V1
 model: Scalance W744-1PRO
Scalance W788-1PRO
Scalance W788-2PRO
Scalance W788-1RR
Scalance W788-2RR
Scalance W746-1PRO
Scalance W747-1RR

Intended use Wireless Communication

Complies with the essential requirements of Article 3 of the R&TTE 1999/5/EC Directive, if used for its intended use and that the following standards have been applied:

1. Safety (Article 3.1.a of the R&TTE Directive)	
Applied standard(s)	issue
<u>EN 60950</u>	<u>2000</u>
2. Electromagnetic compatibility (Article 3.1.b of the R&TTE Directive)	
Applied standard(s)	issue
<u>EN 301489-1 V1.4.1</u>	<u>2002-08</u>
<u>EN 301489-17 V1.2.1</u>	<u>2002-08</u>
3. efficient use of the radio frequency spectrum (Article 3.2 of the R&TTE Directive)	
Applied standard(s)	issue
<u>EN 300 328-2 V1.2.1</u>	<u>2001-12</u>
<u>EN 301 893 V1.2.3</u>	<u>2003-08</u>
4. Health (Article 3.1a of the R&TTE Directive)	
Applied standard(s)	issue
<u>EN 50 392</u>	<u>2002</u>
<u>1999/519/EC</u>	

Nuremberg 7.03.2005
 (Place and Date)

Herian
 (Name and Signature)

ATEX, cULus and FM Approvals

The products

SIMATIC NET SCALANCE W788-1PRO

SIMATIC NET SCALANCE W788-2PRO

SIMATIC NET SCALANCE W788-1RR

SIMATIC NET SCALANCE W788-2RR

has the following approvals

- EN50021
- UL 60950-1
- FM Hazardous (Classified) Location Electrical Equipment:
Non Incendive / Class I / Division 2 / Groups A,B,C,D / T* and
Non Incendive / Class I / Zone 2 / Group IIC / T*

(T* = For concrete information on the temperature class, refer to the type plate)



Warning

When used under hazardous conditions (Zone 2), the SCALANCE W78x product must be installed in an enclosure. To comply with EN 50021, this enclosure must meet the requirements of at least IP 54 in compliance with EN 60529.

DO NOT CONNECT OR DISCONNECT EQUIPMENT UNLESS AREA IS KNOWN TO BE NONHAZARDOUS.

Note

The specified approvals apply only when the corresponding mark is printed on the product.

FCC Approval

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

Notice

Changes or modifications made to this equipment not expressly approved by SIEMENS may void the FCC authorization to operate this equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Notice

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Appendix

Private MIB Variables of the SCALANCE W78x

Downloading the MIB of the SCALANCE W78x over the Internet Explorer

Using the URL http://<IP_address>/snScalanceW.mib, you display the login window if you are not yet logged on. After logging on, the private MIB file of the SCALANCE W is available. When you save on your PC, the source text view should be enabled.

OID

The private MIB variables of the SCALANCE W78x have the following object identifiers:

```
iso(1).org(3).dod(6).internet(1).private(4).  
enterprises(1).ad(4196).adProductMibs(1).simaticNet(1).  
iScalanceW(4)
```

Variables

The following table shows the private MIB variables of the SCALANCE W78x:

Name	OID	Description	Number of Objects
snDownload	1.3.6.1.4.1.4196.1.1.4.100.1.5	Download information and control variables for image, configuration file, events table.	17
snNvLog	1.3.6.1.4.1.4196.1.1.4.100.1.6	Log for events.	8
snTrapInfo	1.3.6.1.4.1.4196.1.1.4.100.1.7	Information on traps.	6
snGen	1.3.6.1.4.1.4196.1.1.4.100.1.8	General information, not conforming with MIB-2.	23
snTcpip	1.3.6.1.4.1.4196.1.1.4.100.1.10	IP address, Subnet mask, Default gateway, DHCP status...	5
snScalanceWCommon	1.3.6.1.4.1.4196.1.1.4.100.2.1	SCALANCE W - specific settings.	24
snScalanceWFilter	1.3.6.1.4.1.4196.1.1.4.100.2.4	Protocol filters and storm threshold settings	18
snScalanceWStats	1.3.6.1.4.1.4196.1.1.4.100.2.5	Information on WLAN 1 and WLAN 2 interfaces.	62
snScalanceWDevices	1.3.6.1.4.1.4196.1.1.4.100.2.6	AP mode: List and information on all clients currently "associated" or connected. Client mode: List of devices with which the client is currently connected.	49
snScalanceWScan	1.3.6.1.4.1.4196.1.1.4.100.2.7	Client mode: List of reachable WLANs and information whether the clients can connect to them.	11
snScalanceWAcl	1.3.6.1.4.1.4196.1.1.4.100.2.8	information and settings for the Access Control Lists.	9
snScalanceWAccess	1.3.6.1.4.1.4196.1.1.4.100.2.9	List of IP addresses that can access the management interface.	5
snScalanceWVirtualAp	1.3.6.1.4.1.4196.1.1.4.100.2.10	Information on the currently configured virtual APs.	17

Traps

Name	Specific Index	Variable	Description
snScalanceWPowerLineDown	31	snScalanceWChangedPowerLine - The power line where the last power down occurred. 1-M12, 2-Ethernet Power	This is generated if there is a power down on M12 or the Ethernet power connector.
snScalanceWPowerLineUp	32	snScalanceWChangedPowerLine - The power line where the last power up occurred. 1-M12, 2-Ethernet Power	This is generated if there is a power up on M12 or the Ethernet power connector.
snScalanceWFault	41	snScalanceWFaultValue - Fault value: 0 = no fault, bit 0 = power M12 is off, bit 1 = link down, bit 2 = internal error, bit 23 = Link Check error, bit 24 = IP Alive broken, bit 25 = power ethernet is off, bit 26 = Cold/warm start, bit 27 = C-PLUG error, bit 28 = iQoS error, bit 29 = Redundancy error"	This is generated if the snScalanceWFaultValue variable is changed. The bit is set to "1" according to the event that has occurred.
snScalanceWIQOS	51	snScalanceWIQOSValue - Description of the last snScalanceWIQOS trap	
snScalanceWLinkCheckOff	81	snScalanceWLinkCheckValue - Description of the last snScalanceWLinkCheckOff Trap	This is generated if a timeout occurs with a client monitored with Link Check.
snScalanceWLinkIntegrityOn	82	snScalanceWLinkCheckValue - Description of the last snScalanceWLinkCheckOn trap	This is generated if a client monitored with Link Check logs on again at the AP following a timeout.
snScalanceWClientAuthenticated	85	SnScalanceWClientsIndex - An index of the client in the snScalanceWClients table	This is generated when a client logs on at the AP.
snScalanceWClientDeAuthenticated	86	SnScalanceWClientsIndex - An index of the client in the snScalanceWClients table	This is generated when a client logs off from the AP.
snScalanceWRedundancy	53	SnScalanceWRedundancyValue - Description of the last redundancy trap. SnScalanceWRedundancyState - Status of redundancy connection	This is generated if the status of the redundant connection changes, for example when the connection of wireless interface A aborts.
snScalanceWOverlapAP	101	snScalanceWOverlapAPValue - Description of the last OverlapAP trap.	Is generated when an access point is detected on the device's own or an overlapping wireless channel.

snScalanceWiPCFPNIOmaxSTAs	111	snScalanceWPNIOValue - Description of the last snScalanceWiPCFPNIOmaxSTAs or snScalanceWiPCFPNIOCycleTime trap	Is generated when there are too many clients registered for the specified update time in iPCF mode with PNIO support.
snScalanceWiPCFPNIOCycleTime	112	snScalanceWPNIOValue - Description of the last snScalanceWiPCFPNIOmaxSTAs or snScalanceWiPCFPNIOCycleTime trap	Is generated when the specified update time in iPCF mode with PNIO support cannot be kept to.
snScalanceWForcedRoamingVapStateChanged	121	snScalanceWVirtualApIndex - Index of the VAP snScalanceWVirtualApState - Current State of the VAP unknown (0) authenticated (1) associated (2) powersafe (3) adhoc (4) joined (5) vap-is-up (6) vap-starting (7) vap-is-down (8) locked (9) vap-connected (10)	Generated when the status of the VAP changes.

Designing and Calculating Wireless Systems Based on the Example of RCoax

Calculating in Decibels

Decibels as a Logarithmic Unit of Measure

In wireless technology, most calculations are made in decibels (dB). Decibel means the logarithm of a ratio. Formulated mathematically, this can be shown by the following equation:

$$\text{Decibel value} = 10 * \log (\text{ratio})$$

Using sample calculations, the following decibel values are obtained:

<u>Ratio</u>	<u>Decibel Value</u>
0.001	-30 dB
0.1	-10 dB
0.2	-7 dB
0.4	-4 dB
0.5	-3 dB
1	0 dB
2	3 dB
4	6 dB

As can be seen in the example, halving a value reduces the decibel value by 3 dB. This remains true regardless of the selected reference variable because only the ratio counts. Which reference variable is used can be recognized by the additional letters or numbers following the dimension dB. In acoustics, for example, the threshold of audibility is the reference variable for a value in dB(A).

Power Specifications

Specifying Power in dBm

A commonly used reference variable in wireless technology is a power of 1 mW. Power can then be specified in the decibel milliwatt unit (dBm). The following formula is used:

$$P [\text{dBm}] = 10 * \log (P [\text{mW}] / 1 \text{ mW})$$

This results in the following power specifications in dBm:

0.5 mW	≈	-3 dBm
1 mW	=	0 dBm
2 mW	≈	3 dBm
4 mW	≈	6 dBm
10 mW	≈	10 dBm
100 mW	≈	20 dBm
200 mW	≈	23 dBm
1 W	≈	30 dBm

Using power specifications, it is simple to calculate gain and attenuation. To calculate an entire system, the individual values for gain and attenuation must simply be added.

Transmit Power dBm

The information in the following tables applies to the following SIMATIC NET products:

- Access point SCALANCE W788-1PRO, W788-2PRO, W788-1RR, W788-2RR
- Client module SCALANCE W744-1PRO, W746-1PRO, W747-1RR
- IWLAN/PB Link

Transmit Power in IEEE 802.11b Mode (2.4 GHz)

Data rate [Mb/s]	P ₀ [dBm]
1	18
2	18
5.5	18
11	18

Transmit Power in IEEE 802.11g Mode (2.4 GHz)

Data rate [Mb/s]	P ₀ [dBm]
6	17
9	17
12	17
18	17
24	17
36	13
48	11
54	10

Transmit Power in IEEE 802.11a/h Mode (5 GHz)

Data rate [Mb/s]	P ₀ [dBm]
6	17
9	17
12	17
18	17
24	17
36	13
48	11
54	10

Specifying Power in dBi

If power is specified in dBi, the reference variable is the transmit power of an isotropic antenna or unipole. Such a (hypothetical) antenna radiates energy from a central point uniformly in all directions.

From the directional radiation of a real antenna, a dBi value is obtained known as the antenna gain. This term is misleading in as far as no energy is gained by an antenna in the physical sense. The higher radiation of a passive antenna results solely from the concentration of radiation in a certain direction. In other spatial segments, there is accordingly less power.

Losses Based on the Example of a 2.4 GHz RCoax Cable

Losses due to Longitudinal Attenuation

The longitudinal attenuation of the leaky feeder cable depends on its length and is calculated according to the following formula:

$$a_{rc} = \alpha_{rc} * l$$

a_{rc} Longitudinal attenuation of the cable in dB

α_{rc} Attenuation coefficient in dB/m as specified in the technical specifications of the cable:
RCoax Cable 0.17 dB/m at 2.4 GHz
connecting cable: 0.55 dB/m at 2.4 GHz

l Total length of the cable in m

The values for the RCoax cable can be found in the technical specifications in Chapter 7.

Losses due to Coupling Loss

Coupling loss c_d includes the losses at the transition from the cable to the surrounding space. The coupling loss depends on the construction of the cable and its physical properties. Values for coupling loss are therefore specified for the particular cable in the technical specifications.

Losses Due to Spatial Attenuation

Spatial attenuation a_{fr} specifies the attenuation between the RCoax cable and the communications partner. The decisive factor here is therefore the distance between the RCoax cable and communication partner. The following formula is used:

$$a_{fr} = 20 * \log(4\pi d / \lambda)$$

a_{fr} Spatial attenuation in dB.

d Distance between cable and antenna in m.

λ Wavelength of the electromagnetic oscillation in m; at a frequency of 2.4 GHz, the wavelength is 0.125 m.

Note

The formula is valid only for the 2.4 GHz RCoax cable.

IEC 61196-4

Values for coupling losses according to IEC 61196-4 already include spatial attenuation of 2 m. To calculate the actual coupling loss, a spatial attenuation for the distance of 2 m must be deducted from this value. The coupling loss for a specified distance between the RCoax cable and the antenna of the communication partner is therefore calculated according to the following formula:

$$c_d = c_{95} - 20 \cdot \log(4\pi \cdot 2\text{m} / \lambda) + 20 \cdot \log(4\pi d / \lambda)$$

c_d Coupling loss of the cable in dB for a specified distance between cable and antenna.

c_{95} c_{95} value of the coupling loss (specified in the data sheet of the cable)

λ Wavelength of the electromagnetic oscillation in m; at a frequency of 2.4 GHz, the wavelength is 0.125 m.

d Distance between cable and antenna in m.

For a frequency of 2.4 GHz, you can also calculate with the following equation in which you must specify the distance d in meters:

$$c_{d \text{ 2.4 GHz}} = c_{95} - 46 \text{ dB} + 20 \cdot \log(100 \cdot d)$$

For a SIEMENS SIMATIC NET IWLAN RCoax Cable PE 1/2" 2.4 GHz ($c_{95} = 69$ dB at 2.4 GHz), for example, this results in the following coupling losses:

<u>Distance</u>	<u>Coupling loss</u>
1 m	63 dB
2 m	69 dB
5 m	77 dB
10 m	83 dB
100 m	103 dB

Note

The formula is valid only for the 2.4 GHz RCoax cable.

Losses due to Power Splitters

Normally, when a double power splitter is used (one input, two outputs, for example, RCoax N-Connect Female Power Splitter 2-Way) a loss of **3 dB** must be taken into account.

Receiver Sensitivity

The receiver sensitivity is the minimum power that must be fed to a receiver to allow communication to take place. The receiver sensitivity is a device-specific property and depends on the transmission technique and data rate. The information in the following tables applies to the following SIMATIC NET products:

- Access point SCALANCE W788-1PRO, W788-2PRO, W788-1RR, W788-2RR
- Client module SCALANCE W744-1PRO, W746-1PRO, W747-1RR
- CP 7515, CP 1515
- IWLAN/PB Link

Receiver Sensitivity in IEEE 802.11b Mode (2.4 GHz)

Data rate [Mb/s]	P_e [dBm]
1	-90
2	-90
5.5	-90
11	-84

Receiver Sensitivity in IEEE 802.11g Mode (2.4 GHz)

Data rate [Mb/s]	P_e [dBm]
6	-87
9	-86
12	-85
18	-83
24	-80
36	-76
48	-71
54	-66

Receiver Sensitivity in IEEE 802.11a/h Mode (5 GHz)

Data rate [Mb/s]	P _e [dBm]
6	-87
9	-86
12	-85
18	-83
24	-80
36	-76
48	-71
54	-66
72 [*]	-73
96 [*]	-68
108 [*]	-63

[*] Turbo mode

System Calculation Based on the Example of RCoax

Procedure

The calculation of the entire system shows whether communication is possible at the desired transmission rate using the desired components. All losses (longitudinal attenuation, spatial attenuation, power splitters etc.) are deducted from the transmit power. An antenna gain is added. The result is the power fed to a receiver. This power must be higher than the receiver sensitivity. The calculation can be made with the following formula:

$$P_e = P_0 - a_{rc} - c_d - a_{ps} + G_{ANT} - \Delta_{rc} - \Delta_{fr} > P_{e \min}$$

P_e Receiver input power in dBm

P₀ Transmit power in dBm

a_{rc} Longitudinal attenuation of the RCoax cable and the feeder in dB

c_d Coupling loss for the distance between RCoax cable and communication partner (see Section 0)

a_{ps} Power splitter losses in dB

G_{ANT} Antenna gain in dB

Δ_{rc} Correction value for the longitudinal attenuation in dB. Depending on the concrete operating conditions, between 5 and 15 dB.

- Δ_{fr} Correction value for the spatial attenuation in dB. Depending on the concrete operating conditions, between 0 and 20 dB.
- $P_{e\ min}$ Receiver sensitivity in dBm

Glossary

ACL	Access Control List. List with MAC addresses with the right to access the wireless network
Ad hoc network	Wireless network between individual devices (point-to-point)
AES	Advanced Encryption Standard, Encryption according to the Rijndael algorithm.
ARP	Address Resolution Protocol
DFS	Dynamic Frequency Selection. With the Dynamic Frequency Selection function (DFS), that is also part of the 802.11h expansion, an automatic channel change is possible if another user or technical device is discovered on a channel during operation. This includes, for example, radar systems that also use the 5 GHz frequency band. Before a channel is used, it is checked to make sure that no other system is already using the channel or frequency range. If another user is discovered, data transmission on the channel is stopped and there is a change to a different channel. This avoids influence resulting from WLAN systems operating according to 802.11a in the 5 GHz band.
DHCP	Dynamic Host Configuration Protocol
EAP	Extensive Authentication Protocol. Authentication protocol.
ECM	Ethernet-Client-Module
Hidden node problem	Two nodes are arranged in a wireless cell so that they are outside the transmission range of the other station. If they both access the medium at the same time, collisions result.

IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 2 Mbps.
IEEE 802.11a	Standard for wireless networks in the 5 GHz range with transmission rates of up to 54 Mbps.
IEEE 802.11b	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 11 Mbps.
IEEE 802.11g	Standard for wireless networks in the 2.4 GHz range with transmission rates of up to 54 Mbps.
IEEE 802.11h	The IEEE 802.11a standard expanded by TPC and DFS.
IEEE 802.11i	Among other things, the standard describes the WPA2 method, the TKIP procedure and the AES encryption algorithm. IEEE 802.11i removes a series of weak points in the WEP security mechanism.
IEEE 802.1x	The heart of the standard is the use of a Radius server as the authentication server. In addition to this, in IEEE 802.1x, the entire communication is encrypted.
iPCF	i ndustrial P oint C oordination F unction. This function ensures that the entire data traffic of a cell is ordered, controlled by the access point. By avoiding collisions, the throughput can be optimized even with large numbers of nodes. iPCF also allows fast cell changes.
PST	P rimary S etup T ool
RADIUS	R emote A uthentication D ial - U ser S ervice for secure communication networks
Roaming	Free movement of wireless LAN nodes even beyond the boundaries of an access point's cell. The nodes and can move from one cell to the next without any noticeable interruption.
RTS/CTS	R esult t o s end/ C lear t o s end. Scheme for avoidance of collisions.

SSID	Service Set Identifier (SSID) is used to identify a wireless network based on IEEE 802.11
SNMP	Simple Network Management Protocol. Standardized protocol for transporting network management information.
TKIP	Temporal Key Integrity Protocol. Scheme for cyclic changing of keys in WLANs.
TPC	The Transmit-Power Control function (TPC) introduced as a supplementary function by the 802.11h expansion for 5 GHz components allows an automatic adaptation of the transmit power. Information on the attenuation values and the expected budget reserves in received power are taken into account. TPC is also intended to make sure that the maximum permitted transmit power of a channel specified by the relevant regulatory bodies is not exceeded by the component. TPC attempts to operate with the minimum transmit power between the communicating stations or between access point and station.
VAP	Virtual Access Point. By using virtual access points, various SSIDs (maximum of 8 per WLAN interface) can be configured with different security settings. You can assign each virtual AP to a particular VLAN.
WBM	Web Based Management. HTTP-based configuration method in which an HTTP server is used in the SCALANCE W78x.
WDS	Wireless Distribution System. Radio links for connecting the access points for an extended service set (ESS)
WEP	WEP (Wired Equivalence Privacy) is an optional part of the IEEE 802.11 standard. WEP specifies methods of authentication and encryption working with fixed keys stored on the device. All devices that want to access a network in which WEP is used must first be supplied with the same keys. WEP works with key lengths between 40 and 128 bits. Occasionally different key lengths are encountered (for example 256 bits) but these are not intended in the vendor-independent WLAN standards IEEE 802.11b and 802.11g. The keys can only be changed manually.
Wi-Fi	Wireless Fidelity. The Wi-Fi Alliance is a group of WLAN manufacturers that tests and certifies the interoperability of WLAN products. Wi-Fi is a certification of WLANs according to 802.11b and is performed by the WECA of the WiFi parent organization. This certification confirms the interoperability of WLAN products operating

in compliance to the 802.11b standard.

The Wi-Fi Alliance also develops standards. The WiFi Alliance has developed its own architectures for security procedures that have not yet been standardized such as the WiFi Protected Architecture (WPA) to be able to test the compatibility of the various manufacturers' products.

For real-time transmission, the Wi-Fi Alliance has specified Wi-Fi Multimedia (WMM) for transmissions with guaranteed quality of service (QoS).

WMM

Wi-Fi Multimedia

WPA

WPA (Wi-Fi Protected Access) is a method specified by the Wi-Fi Alliance to close security gaps in WEP. Authentication using a server is stipulated (802.1x). The dynamic exchange of keys at each frame introduces further security. As the encryption method, you can choose between TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard).

Although WPA never became an official component of the IEEE 802.11 family of standards, it has become very widespread in a short time. This, however, applies only to the WPA procedure described above using TKIP. The optional possible implementation of WPA on the basis of AES, on the other hand, did not become established and is therefore irrelevant in everyday practice. AES only took on practical value only with the development of the later WPA2 standard.

WPA-PSK

WPA-PSK is a weakened form of WPA. In this method, authentication is not established by a server but is based on a password. This password must be configured manually on the client and server. Wherever possible, you should change to the WPA method to achieve greater security.

Index

A

ACL.....	174
Ad Hoc networks	14
Adopt MAC Address.....	69
Antennas	34, 151
ARP table	192
Auth Log	228
Authentication.....	84, 163

B

Bandwidth reservation.....	213
Basic Wizard.....	61, 63
Beacon	149
Bridge	180

C

Channel Selection	72
CLI commands	
shortcuts for commands	102
symbolic representation.....	103
Client List.....	230
Command Line Interface	102
C-PLUG	28, 136

D

Decibel.....	261
DHCP server	112
DLC protocol.....	48
installation	49

E

E-mail	121
Encryption.....	86, 165

F

Forward delay	195
---------------------	-----

H

Hello Time	195
Help function.....	101
HiPath.....	106
HTTPS.....	60
Hybrid cable.....	35

I

IEEE 802.11a	23
--------------------	----

IEEE 802.11b.....	23
IEEE 802.11g.....	23, 157
IEEE 802.11h.....	23
IP address.....	63
IP, TCP/IP, ICMP, SNMP	242
IP-Alive.....	224
iPCF	93, 215
iPCF Wizard.....	61, 93
iQoS	238
iQoS	213

L

Learning Table	192
LED simulation.....	100
Lightning Protection	31
Link Check	220
Locale setting.....	104
Log table	227
Losses.....	264

M

MAC filter	210
Max Age	195
Multichannel configuration	16

N

NAT	203
New	101

O

Overlap AP.....	236
-----------------	-----

P

Password	76
Path cost	197
Power specifications	262
Power Supply.....	33
PRESET PLUG.....	44
Primary Setup Tool	
Installation	51
via command line	56
Priority	196
Protocol filter	212

R

RADIUS	88, 178
--------------	---------

Receiver sensitivity	266
Redundant connection	222
Refresh	101
RTS/CTS	149, 152
S	
Save	
Device data	132
Security settings	79
Security Wizard	61, 75
Set values	101
SNMP	122
SNTP	130
Spanning Tree	192, 240
Spanning tree port parameters	196
SSID	80
Standalone configuration	13
Storm threshold	202
Suppress SSID broadcasting	167
T	
Transmit power	149
TTL	112
V	
Versions	229
W	
WDS	181
Web Based Management	57
WEP	87
Wireless access	15
Wizards	57
WPA	167
WPA2	90